العدد أربعون
تاريخ الإصدار: 2 – شباط – 2022 م
www.ajsp.net
ISSN: 2663-5798

"مدى وعي طلبة الدراسات العليا بنظام مكافحة الجرائم المعلوماتية في ظل التحول الرقمي ضمن رؤية المملكة ٢٠٣٠: دراسة مسحية لدى طلبة كلية الآداب والعلوم الانسانية بجامعة الملك عبدالعزيز بجدة"

إعداد الباحثتان:

شهد عبدالرحمن الصبحي

باحثة في قسم إدارة المعلومات – كلية الأدب والعلوم والإنسانية

جامعة الملك عبدالعزيز

د. ريم علي الرابغي

أستاذ مشارك في قسم عام المعلومات – كلية الأدب والعلوم والإنسانية

جامعة الملك عبدالعزيز

العدد أربعون
تاريخ الإصدار: 2 – شباط – 2022 م
www.ajsp.net
ISSN: 2663-5798

ملخص البحث:

هدفت الدراسة إلى التعرف على مدى الوعي بنظام مكافحة الجرائم المعلوماتية السعودي في ظل التحول الرقمي ضمن رؤية 2030 لدى طلاب وطالبات الدراسات العليا بكلية الآداب والعلوم الانسانية في جامعة الملك عبدالعزيز، من خلال التعرف على مدى وعيهم بالجرائم المعلوماتية المذكورة في النظام، ورصد مدى وعيهم بأدوات الإبلاغ عن الجرائم المعلوماتية في السعودية، وإيضاح أسباب ضعف الوعي بالنظام، والكشف عن طرق المكافحة والوقاية من الجرائم المعلوماتية في ظل التحول الرقمي تماشياً مع رؤية 2030 حسب وجهة نظرهم. واعتمدت الدراسة على المنهج الوصفي المسحي من خلال أداة جمع البيانات الاستبانة وقد بلغت عينة الدراسة من (317) طالباً وطالبة. وتوصلت الدراسة إلى عدد من النتائج، أهمها: أن مستوى الوعي بالجرائم المعلوماتية المذكورة بنظام مكافحة الجرائم المعلوماتية السعودي قد بلغ درجة مرتفعة لدى أفراد عينة الدراسة، بمتوسط حسابي قدره (2.79). وكشفت الدراسة عن أسباب ضعف الوعي بنظام مكافحة جرائم المعلوماتية السعودي حسب وجهة نظر أفراد عينة الدراسة ومن الأسباب الأكثر أثراً هو قلة اهتمام أفراد المجتمع بنظام مكافحة جرائم المعلوماتية من خلال الاطلاع عليه ومعرفة مدى أهميته، كما كشفت عن أبرز طرق المكافحة والوقاية من الجرائم المعلوماتية في ظل التحول الرقمي تماشياً مع رؤية 2030 حسب وجهة نظر أفراد عينة الدراسة ومن أهمها تطوير برمجيات آمنة ونظم تشغيل قوية التي تحد من الاختراقات الالكترونية، كما أظهرت الدراسة إلى أن مستوى المعرفة والوعي بأدوات الإبلاغ عن الجرائم المعلوماتية في المملكة العربية السعودية قد بلغ درجة متوسطة لدى أفراد عينة الدراسة، بمتوسط حسابي قدره (2.14). ومن أهم توصيات الدراسة ضرورة تطوير وتحديث نظام مكافحة الجرائم المعلوماتية السعودي بشكل مستمر ليواكب كافة أنواع الجرائم المعلوماتية وأنماطها الناشئة والمستحدثة، كما ينبغي على الجهات المختصة القيام بمبادرات توعوية تساهم في توعية أفراد المجتمع بما يتعلق بالجرائم المعلوماتية وأنظمة مكافحتها بشكل دوري ومستمر لرفع مستوى ثقافة المجتمع.

الكلمات المفتاحية: الجرائم المعلوماتية، نظام مكافحة الجرائم المعلوماتية، التحول الرقمي، أمن المعلومات، رؤية 2030

أولاً: الإطار المنهجي

1. المقدمة

يشهد العصر الرقمي في العالم المعاصر تطورات متلاحقة وقد عمدت معظم دول العالم لرسم خطط وبرامج للتحول الرقمي، ودعم ذلك برسم رؤى مستقبلية تعزز الإجراءات والعمليات اللازمة لتحقيقها، وأصبح يتكرر مصطلح الرقمنة الذي اتجهت معظم الطروحات لصياغة متطلباته، وقد شغلت التطورات المتسارعة في قطاع تقنية المعلومات والاتصالات حيزاً لا يستهان به في ذهن الأفراد وأداء المنظمات الحيوية ونادت معظم الآراء في مجال التقنية الرقمية بضرورة تلبية مجموعة من المقومات لتحسين جودة العمل وتعزيز التنافسية وتحقيق التنمية المستدامة وهي: السرعة والدقة والجودة وأمن المعلومات.

وفي الجانب الآخر وكأي تقنية واختراع هناك جوانب إيجابية وجوانب سلبية قد تنتج هذه الأخيرة من سوء استخدام التقنيات والأنظمة المعلوماتية والذي قد يمتد إلى استخدامها بشكل يتسبب في حدوث ضرر لمصالح الأفراد أو المنظمة وهذا ما يؤكده ظهور أشكالاً حديثة من الجرائم التي أطلق عليها الجرائم المعلوماتية.

وأخذت هذه الجرائم المعلوماتية في التوسع والانتشار وأدى ذلك إلى تزايد خطرها مع انتشارها بشكل كبير، حيث أصبحت المملكة العربية السعودية أمام تحدي تمثل في ظهور الجرائم المعلوماتية التي تستهدف المجتمع.

العدد أربعون
تاريخ الإصدار: 2 – شباط – 2022 م
www.ajsp.net
ISSN: 2663-5798

وفي ضوء ذلك بادرت المملكة العربية السعودية إلى إصدار نظام مكافحة جرائم المعلوماتية وذلك بقرار من مجلس الوزراء برقم 79 / وتاريخ 7/ 3/ 1428 هـ وتمت المصادقة عليه بموجب المرسوم الملكي الكريم رقم م/ 17 وتاريخ 8/ 3/ 1428 هـ. ويهدف هذا النظام إلى تقليص حجم الجرائم المعلوماتية، وذلك بفرض العقوبات للحد منها، إذ يسعى النظام للوصول إلى الأمن المعلوماتي وتحقيقه والحفاظ على الحقوق الناتجة عن الاستخدام القانوني لتقنية المعلومات، كما لابد من تحقيق التوازن بين مصلحة الفرد والمجتمع في تطبيق التقنيات الرقمية الحديثة.

ومن هذا المنطلق جاءت أهمية إجراء الدراسة لمعرفة مدى الوعي بنظام مكافحة الجرائم المعلوماتية السعودي في ظل التحول الرقمي ضمن رؤية 2030 لدى طلاب وطالبات الدراسات العليا بكلية الآداب والعلوم الانسانية في جامعة الملك عبدالعزيز بجدة، وذلك باعتبار أنهم أحد فئات المجتمع الذي يستهدفهم النظام لحمايتهم.

2. مشكلة الدراسة:

مع التطورات الحديثة وتوجه المملكة العربية السعودية والسعي إلى تحقيق التحول الرقمي ضمن رؤية 2030 على كافة الأصعدة ولجميع قطاعاتها، لوحظ ظهور عدد كبير من الجرائم المعلوماتية المستحدثة في الوقت الحاضر حيث تحتاج هذه الجرائم إلى جهود من أجل مكافحتها وضبط تمددها لأنها جرائم عابرة للحدود ويصعب إثباتها، وتعتبر المملكة العربية السعودية أحد الدول المساهمة للحد من وقوع الجرائم المعلوماتية. فقد أصدرت نظام مكافحة جرائم المعلوماتية الذي يسعى للوصول إلى الأمن المعلوماتي وتحقيقه والحفاظ على الحقوق الناتجة عن الاستخدام القانوني للحاسبات والشبكات المعلوماتية. وبناءً على ذلك دعت الحاجة إلى إجراء الدراسة الحالية وذلك لإثراء وتوعية الطلاب والطالبات بنظام مكافحة جرائم المعلوماتية تجنباً من الوقوع في الجرائم المعلوماتية وتعرضهم لها.

وتتلخص مشكلة الدراسة في السؤال الآتي: ما مدى الوعي بنظام مكافحة الجرائم المعلوماتية السعودي في ظل التحول الرقمي ضمن رؤية 2030 لدى طلاب وطالبات الدراسات العليا بكلية الآداب والعلوم الانسانية في جامعة الملك عبدالعزيز ؟

3. أهداف الدراسة:

تهدف الدراسة بشكل رئيسي إلى التعرف على مدى الوعي بنظام مكافحة الجرائم المعلوماتية السعودي في ظل التحول الرقمي ضمن رؤية 2030 لدى طلاب وطالبات الدراسات العليا بكلية الآداب والعلوم الانسانية في جامعة الملك عبدالعزيز، وبناءً عليه تتدرج عدة أهداف فرعية؛ وهي على النحو الآتي:

1- التعرف على مدى الوعي بالجرائم المعلوماتية المذكورة في نظام مكافحة الجرائم المعلوماتية السعودي لدى طلاب وطالبات الدراسات العليا بكلية الآداب والعلوم الإنسانية في جامعة الملك عبدالعزيز.
2- إيضاح أسباب ضعف الوعي بنظام مكافحة جرائم المعلوماتية من وجهة نظر طلاب وطالبات الدراسات العليا بكلية الآداب والعلوم الإنسانية في جامعة الملك عبدالعزيز.
3- الكشف عن طرق المكافحة والوقاية من الجرائم المعلوماتية في ظل التحول الرقمي تماشياً مع رؤية 2030 من وجهة نظر طلاب وطالبات الدراسات العليا بكلية الآداب والعلوم الإنسانية في جامعة الملك عبدالعزيز.
4- التعرف على مدى الوعي بأدوات الإبلاغ عن الجرائم المعلوماتية في المملكة العربية السعودية لدى طلاب وطالبات الدراسات العليا بكلية الآداب والعلوم الإنسانية في جامعة الملك عبدالعزيز.

العدد أربعون
تاريخ الإصدار: 2 – شباط – 2022 م
www.ajsp.net
ISSN: 2663-5798

4. أهمية الدراسة:

تستمد الدراسة أهميتها من أهمية موضوعها وحداثته، إذ اتجهت المملكة العربية السعودية إلى تبني مفهوم التحول الرقمي تماشياً مع رؤية 2030. وسعت كافة المؤسسات والهيئات المختلفة إلى تحسين خدماتها وتعاملاتها بشكل إلكتروني لمواكبة هذا التحول الرقمي، مما أدى هذا التطور إلى جوانب سلبية ملازمة له وهي الجرائم المعلوماتية التي تؤثر سلباً على استخدام تقنية المعلومات. ومن هنا تأتي أهمية نظام مكافحة جرائم المعلوماتية الذي أصدرته المملكة العربية السعودية للحد من وقوع هذه الجرائم والمساعدة على تحقيق الأمن المعلوماتي. ويعد الوعي بنظام مكافحة الجرائم المعلوماتية مطلباً ملحاً لضمان تطبيقه.

حيث تساهم الدراسة الحالية في إثراء وتوعية الطلاب والطالبات بنظام مكافحة جرائم المعلوماتية للحد من الوقوع في الجرائم المعلوماتية. أيضاً العمل على تعزيز دور النظام وتحقيق أهدافه باعتبار أنهم أحد فئات المجتمع الذي يستهدفهم النظام لحمايتهم.

وتعد الدراسة من أوائل الدراسات التي تناولت قياس الوعي بنظام مكافحة الجرائم المعلوماتية السعودي لدى طلاب وطالبات الدراسات العليا في كلية الآداب والعلوم الإنسانية بجامعة الملك عبدالعزيز، كما أنها من الدراسات التي تسعى للإضافة في الإنتاج الفكري وتعزيز المحتوى العربي.

5. تساؤلات الدراسة:

تسعى الدراسة في سبيل تحقيق أهدافها إلى الإجابة على التساؤلات الآتية:

1- ما مدى الوعي بالجرائم المعلوماتية المذكورة في نظام مكافحة الجرائم المعلوماتية السعودي لدى طلاب وطالبات الدراسات العليا بكلية الآداب والعلوم الإنسانية في جامعة الملك عبدالعزيز؟

2- ماهي أسباب ضعف الوعي بنظام مكافحة جرائم المعلوماتية من وجهة نظر طلاب وطالبات الدراسات العليا بكلية الآداب والعلوم الإنسانية في جامعة الملك عبدالعزيز؟

3- ماهي طرق المكافحة والوقاية من الجرائم المعلوماتية في ظل التحول الرقمي تماشياً مع رؤية 2030 من وجهة نظر طلاب وطالبات الدراسات العليا بكلية الآداب والعلوم الإنسانية في جامعة الملك عبدالعزيز؟

4- ما مدى الوعي بأدوات الإبلاغ عن الجرائم المعلوماتية في المملكة العربية السعودية لدى طلاب وطالبات الدراسات العليا بكلية الآداب والعلوم الإنسانية في جامعة الملك عبدالعزيز؟

6. مجال الدراسة وحدودها

يتمثل مجال الدراسة وحدودها في الحدود الآتية:

- **الحدود المكانية:** اقتصرت الحدود المكانية للدراسة على كلية الآداب والعلوم الإنسانية في جامعة الملك عبدالعزيز بمدينة جدة.
- **الحدود الموضوعية:** يغطي المجال الموضوعي للدراسة على دراسة وعي طلاب وطالبات الدراسات العليا بكلية الآداب والعلوم الإنسانية في جامعة الملك عبدالعزيز بنظام مكافحة الجرائم المعلوماتية السعودي.
- **الحدود البشرية:** تغطي الحدود البشرية في هذه الدراسة على طلاب وطالبات الدراسات العليا بكلية الآداب والعلوم الإنسانية في جامعة الملك عبدالعزيز بجدة.
- **الحدود الزمنية:** تطبيق وإجراء الدراسة خلال الفصل الدراسي الأول للعام الجامعي 1443هـ – 2021م.

7. منهج الدراسة وأداتها:

اتبعت الدراسة المنهج الوصفي المسحي، وذلك لملائمته لطبيعة الدراسة ومجال تطبيقها، والتي تهدف لمعرفة مستوى الوعي بنظام مكافحة الجرائم المعلوماتية السعودي في ظل التحول الرقمي ضمن رؤية 2030 لدى طلاب وطالبات الدراسات العليا بكلية الآداب والعلوم الانسانية في جامعة الملك عبدالعزيز. واعتمدت الدراسة على أداة الاستبانة لجمع المعلومات والبيانات اللازمة، لمناسبتها للمنهج المتبع في الدراسة، والأكثر ملائمة لتحقيق أهدافها والإجابة على تساؤلاتها.

ويتمثل مجتمع الدراسة من جميع طلاب وطالبات الدراسات العليا الفعالين خلال الفصل الدراسي الأول للعام الجامعي 1443هـ – 2021م بكلية الآداب والعلوم الإنسانية في جامعة الملك عبدالعزيز، والبالغ عددهم (1829) طالباً وطالبة، وفقاً للإحصائيات الرسمية التي تم الحصول عليها من عمادة الدراسات العليا في جامعة الملك عبدالعزيز بجدة. وقد تم أخذ عينة عشوائية ممثلة لمجتمع الدراسة بلغ عددها (317) طالباً وطالبة، وذلك وفق ما حدده جدول كرجسي ومورغان (Krejcie & Morgan, 1970).

8. مصطلحات الدراسة:

تناولت الدراسة مجموعة من المصطلحات والمفاهيم الذي تم توظيفها إجرائياً لمتطلبات العمل وفقاً للنحو الآتي:

1) الجريمة المعلوماتية (Cybercrime):

وهي عبارة عن كل سلوك أو إجراء أو عملية غير قانونية تتم من خلال استخدام الأجهزة الرقمية وتوظيف التقنيات والبرامج للحصول على مجموعة فوائد معنية أو مادية لتحقيق أهداف غير مشروعة مثل السرقة والقرصنة أو استغلال للمعلومات على نحو سلبي.

2) نظام مكافحة جرائم المعلوماتية (Anti-Cybercrime Law):

هو حزمة من المصطلحات والتشريعات والأعراف والعقوبات ومجموعة من المبادئ المعتمدة لمكافحة الجرائم المعلوماتية صدر بموجب المرسوم الملكي رقم م/17 وتاريخ 1428/3/8 هـ.

3) **التحول الرقمي (Digital Transformation):**

تعددت المفاهيم التي تحاول أن تشرح مفهوم التحول الرقمي وهو الذي يقوم في محوره على الانتقال من النواحي التقليدية إلى توظيف التقنيات الرقمية وتوظيف ذلك في تناول البيانات وتطوير نماذج الأعمال ذات الطابع الرقمي.

4) رؤية 2030 (Vision 2030):

وهي تصور وطني طويل المدى يهدف إلى تحقيق تنمية شاملة في المملكة العربية السعودية ودعمها لتكوين نموذجاً ذا ريادة عالمية من خلال التمكين وتعزيز القدرات ودعم الطاقات لأفراد المجتمع واستثمار نقاط القوة لخلق اقتصاد متنوع ومزدهر وبناء مجتمع حيوي ينعم بحياة عامرة صحية (رؤية 2030، 2021).

9. الدراسات السابقة:

يتم في هذا في السياق استعراض مجموعة من الدراسات العلمية العربية والأجنبية ذات العلاقة بالمجال الموضوعي للدراسة الحالية، ومعتمدة في عرضها على الترتيب الزمني من الأحدث إلى الأقدم.

أولاً: الدراسات العربية:

- **دراسة عبدالرزاق (2021) بعنوان "تأثير الذكاء الاصطناعي على الجريمة الالكترونية"** سعت الدراسة إلى تتبع تأثير استخدامات الذكاء الاصطناعي على ارتكاب الجرائم المعلوماتية، مناقشة موقف التشريع السعودي والمصري المرتبط بمكافحة جرائم المعلومات. واستندت الدراسة على المنهج الوصفي التحليلي والمنهج المقارن. توصلت بمجموعة من النتائج منها أن الذكاء الاصطناعي ساهم في زيادة الجرائم الإلكترونية وانتشارها؛ وتجريم النظام السعودي والقانون المصري للجريمة الإلكترونية في نصوص مستقلة عن النصوص القانونية للجرائم التقليدية؛ مواكبة النظام السعودي والقانون المصري للتشريعات المقارنة في ملاحقتها للأنماط المستحدثة من الجريمة الالكترونية؛ حدد النظام السعودي معظم الأفعال التي تشكل خطرًا على المعلومات وجعلها من الجرائم المعلوماتية، ووضح عقوبة الشروع في تلك الجرائم. وقد أوصت الدراسة بالعمل على تطبيق أنظمة حماية المعلومات ومراجعتها بصورة دورية لتطويرها بما يتناسب مع سرعة التقدم التقني؛ وضرورة التعاون الدولي لمكافحة الجرائم الإلكترونية من خلال الاتفاقيات الدولية والإقليمية؛ كما يجب نشر الوعي بين المواطنين وخاصةً الشباب بمخاطر التعامل مع المواقع السيئة والمشبوهة عبر شبكة الانترنت.
- **دراسة المطوع (2021) بعنوان "مستوى الوعي لدى طلبة كلية التربية بشقراء بجامعة شقراء بنظام مكافحة جرائم المعلوماتية والتدابير التربوية لزيادته"** اكتشفت الدراسة مستوى الوعي لدى طلبة كلية التربية بجامعة شقراء بنظام مكافحة جرائم المعلوماتية للتعرف على التدابير التربوية التي يمكن أن تتبعها الكلية لزيادة مستوى الوعي. واستخدمت الدراسة أكثر من منهج وهو المنهج الوصفي والمسحي والاستقرائي واعتمدت على أداة الاستبانة. وقد أظهرت الدراسة موافقة أفراد العينة على عبارات محاور الدراسة، وقد بلغ المتوسط الحسابي العام للمحاور على التوالي(4.02) (3.71) (3.81) وهي قيمة منخفضة نسبياً تظهر الحاجة لزيادة مستوى الوعي لدى الطلبة بنظام مكافحة جرائم المعلوماتية. ولعل من أهم ما يحقق زيادة الوعي ضرورة نشر الوعي بالمخاطر المترتبة على الاستخدام غير الآمن، ومن ثم إتاحة الفرصة للمواطنين وخصوصاً الشباب للمشاركة في مكافحة جرائم المعلوماتية. كما أظهرت الدراسة عدد من التدابير التربوية التي يمكن اتخاذها لزيادة مستوى الوعي ومن ذلك تبصيرهم بماهية الجرائم المعلوماتية وبأخطارها وبأهم الطرق لمواجهتها. وقد أوصت الدراسة بضرورة إجراء دراسات علمية لمعرفة مستوى وعي الطلبة باللوائح والأنظمة الوطنية المشابهة لنظام مكافحة جرائم المعلوماتية. وإجراء دراسات علمية متخصصة تقنياً وقانونياً واجتماعياً وتربوياً بشكل مستمر لمعرفة مستوى فاعلية نظام مكافحة جرائم المعلوماتية وتقديم تغذية راجعة علمية لتطوير النظام.
- **دراسة الخطيب (2019) بعنوان "الجرائم المعلوماتية عبر مواقع التواصل الاجتماعي قراءة في قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة ٢٠١٨ ونظام مكافحة جرائم المعلوماتية السعودي ١٤٢٨هـ"** هدفت الدراسة إلى توضيح الجرائم المعلوماتية التي تستخدم مواقع التواصل الاجتماعي، وبيان موقف كلاً من المشرع المصري والمنظم السعودي اتجاه جرائم تقنية المعلومات. واعتمدت الدراسة على المنهج التحليلي. ومن أبرز النتائج التي توصلت إليها الدراسة تعد مواقع التواصل الاجتماعي أداة ممتازة لجمع المعلومات؛ لأنها تتضمن معلومات مهمة عن المستخدمين وبالتالي يمكن للشرطة استخدامها في جمع الاستدلالات عن جرائم المعلومات. وتتجسد أول طرق مكافحة الجرائم المرتكبة عبر الانترنت ووسائل التواصل الاجتماعي في الاستدلال الذي يتضمن كل من التفتيش والخبرة. وأوصت الدراسة ضرورة انشاء جهات متخصصة لمكافحة كافة الجرائم الواقعة عبر مواقع التواصل الاجتماعي، كما تحث المشرع المصري والمنظم السعودي بضرورة القيام بتدريب كافة أجهزة الشرطة على الأنظمة المعلوماتية لمواجهة الجرائم المعلوماتية.

- **دراسة سعيد (2019) بعنوان " الوعي المجتمعي بالجرائم المعلوماتية لدى الطالبة الجامعية: دراسة من منظور تنظيم المجتمع في الخدمة الاجتماعية"** عمدت الدراسة إلى التعرف على مستوى الوعي المجتمعي بالجرائم المعلوماتية لدى الطالبة الجامعية من خلال حصر وتحديد أشكال الجرائم المعلوماتية ومخاطرها والتعرف على الأسباب المؤدية لارتكابها. واعتمدت الدراسة على منهج المسح الاجتماعي بالعينة من خلال أداة جمع البيانات الاستبانة. ومن أهم النتائج التي توصلت لها معرفة عينة الدراسة بمصطلح الجرائم المعلوماتية بنسبة 88.3%، وموافقة عينة الدراسة على العوامل المؤدية لارتكاب الجرائم المعلوماتية بمتوسط (2.43 إلى 3) ومن أهمها من وجهة نظرهم ضعف الوازع الديني وزيادة قاعدة مستخدمي الانترنت ونقص وضعف القوانين والتشريعات الرادعة.
- **دراسة الهيف والعنزي(2018) بعنوان "الجرائم المعلوماتية : أنواعها وخطورتها : دراسة لقياس مستوى وعي طالبات قسم المكتبات والمعلومات في جامعة الأميرة نورة بن عبد الرحمن 1438 هـ-1439 2017-2018"** سعت الدراسة إلى قياس الوعي المعلوماتي لدى طالبات قسم المكتبات والمعلومات بجامعة الأميرة نورة، ووضعت مجموعة من الحلول والإجراءات التي تضمن حماية الطالبات من آثار الجرائم المعلوماتية السلبية المترتبة على الوقوع في الجرائم المعلوماتية. وقد اتبعت الدراسة المنهج الوصفي في تحليل البيانات والاحصائيات الدراسة. وقد توصلت الدراسة إلى أن غالبية أفراد العينة لديهم معرفة بوجود نظام مكافحة الجرائم المعلوماتية، ولكن لك يسبق لهم بالاطلاع عليه بنسبة 79%. أن من أهم العناصر التي تساعد في عدم الوقوع في الجرائم المعلوماتية الوعي الديني والأخلاقي، وأن الوقاية من الجرائم المعلوماتية تكون من خلال النشر المكثف لبرامج التوعية. وقد أوصت الدراسة لابد من النشر المكثف لبرامج التوعية عن الجرائم المعلوماتية عن طريق وسائل الاعلام، وتوفير البرامج التي تساعد في الحماية ومنع التجسس وسرقة المعلومات وتمكين الطالبات وتعريفهم كيفية استخدامها، كما يجب بيان مخاطر الجرائم المعلوماتية.
- **دراسة غريب والأمير (٢٠١٧) بعنوان " مدى الوعي لدى الفئة العمرية الشابة بنظام عقوبات الجرائم المعلوماتية السعودي "** هدفت الدراسة إلى معرفة وعي الشباب بمفهوم الجرائم المعلوماتية وأشكالها، ومعرفتهم بنظام العقوبات للجرائم المعلوماتية في السعودية، واعتمدت الدراسة على المنهج المسحي الوصفي من خلال أداة جمع البيانات الاستبانة وقد بلغت عينة الدراسة (214) شاباً وشابة. وقد بينت الدراسة أن غالبية عينة الدراسة ليس لديهم معرفة بنظام العقوبات الخاص بالجرائم المعلوماتية السعودي بنسبة (60.70%)، وأن معرفة الأنظمة وعقوبات مكافحة الجرائم المعلوماتية لدى الشباب الذي تم من خلال الوسائل العلمية المختلفة كان لها دور كبير في الحد من الممارسات السلبية في تقنية المعلومات. وأن وسائل التواصل الاجتماعي هي المصدر الأول للتوعية والاطلاع على المعلومات بالنسبة لعينة الدراسة. وأوصت الدراسة بالطلب من وزارة التعليم إدراج مقرر دراسي خاص بالجرائم المعلوماتية وتوعية مستخدمي تقنية المعلومات بخطرها وعواقبها، أيضاً قيام هيئة الاتصالات وتقنية المعلومات بحملات توعوية مستمرة وهادفة لتوعية المجتمع السعودي. بالإضافة إلى توظيف مواقع التواصل الاجتماعي لنشر رسائل التوعية لمكافحة الجرائم المعلوماتية ونشر الاستخدام الصحيح أجهزة التقنية الحديثة.
- **دراسة أصيل وخضري (2016) بعنوان "مدى الوعي بالجرائم المعلوماتية بين مستخدمي مواقع التواصل الاجتماعي: دراسة مسحية على مدينة جدة"** هدفت الدراسة إلى معرفة وعي مستخدمي مواقع التواصل الاجتماعي بالجرائم المعلوماتية، ومدى وعيهم القانوني، بالإضافة إلى رصد الطرق والأساليب التي يطبقوها للوقاية والحماية من الجرائم المعلوماتية. اتبعت الدراسة المنهج المسحي، واعتمدت على أداة الاستبانة. وقد أظهرت الدراسة إلى عدم وجود معرفة بالقانون السعودي لمكافحة الجريمة المعلوماتية، حيث أشار ما يزيد عن نصف عينة الدراسة وبنسبة (55,6%). وقد أوصت الدراسة بحاجة أفراد المجتمع السعودي لرفع مستوى الوعي القانوني فيما يتعلق بتشريعات المملكة الخاصة بالجرائم المعلوماتية ومكافحتها من حيث وجودها والعمل بها وتطبيقها.

- **دراسة بنوان والمنوفي والجندي (2016) بعنوان "الجامعة وتنمية وعي طلابها بالجرائم الالكترونية في ضوء التطور التقني والمعلوماتي"** هدفت الدراسة إلى معرفة دور جامعة كفر الشيخ في تنمية وعي طلابها بالجرائم الإلكترونية وأنواعها ومخاطرها في ضوء التطورات التقنية والمعلوماتية المعاصرة. واعتمدت الدراسة على المنهج الوصفي. وتوصلت إلى أن دور الجامعة في تنمية وعي طلابها بالجرائم المعلوماتية يتمثل في طرح بعض المقررات مثل مقرر أمن المعلومات، وعقد ندوات في كيفية حماية المعلومات.
- **دراسة متولي (٢٠١٥) بعنوان " الجرائم المعلوماتية (٢,٠): رؤية مقترحة من منظور تربوي لدور أعضاء هيئة التدريس بكليات التربية لزيادة الوعي بمكافحة الجرائم المعلوماتية "** تهدف الدراسة إلى تقديم رؤية مقترحة وإطار من منظور تربوي مستمد من بنية وتنظيم كليات التربية لتفعيل دور أعضاء هيئة التدريس لزيادة الوعي بمكافحة الجرائم المعلوماتية. وتوعية الطلاب بخطورة هذه الممارسات عند استخدامهم تطبيقات الجيل الثاني من الويب. واعتمدت الدراسة على أداة جمع البيانات الملاحظة لرصد بعض الجرائم المعلوماتية. وتوصلت الدراسة إلى عرض إطار مقترح لدور أعضاء هيئة التدريس بكليات التربية من خلال تفاعلهم مع الكيانات التي تشمل وحدات ومراكز ونظم الكليات المختلفة والتي ترتبط بدور أعضاء هيئة التدريس في الوعي بمكافحة الجرائم المعلوماتية. وأوصت الدراسة بضرورة التوسع في نشر برامج الوعي ضد مخاطر الجرائم المعلوماتية والاستخدام الأمن لشبكة الإنترنت، وتوفير مقرر تعليمي على مختلف المراحل التعليمية بمحتوى تعليمي تثقيفي يتم تحديثه بشكل دوري، والتوسع في إجراء الدراسات والبحوث العلمية التي تتناول قضايا تلك الجرائم ومعالجتها وتطبيقها على أرض الواقع.
- **دراسة اليحيى (٢٠١٣) بعنوان " مكافحة جرائم المعلوماتية في المملكة العربية السعودية "** هدفت الدراسة إلى تحديد الجريمة المعلوماتية وأدواتها وعقوباتها من خلال نظام مكافحة جرائم المعلوماتية بالمملكة العربية السعودية حيث ذكر أن طبيعة الجرائم المعلوماتية تختلف عن طبيعة الجرائم التقليدية، فجعل لها خصوصية في أساليبها من الناحية الموضوعية والإجرائية، فأصبحت الحاجة ضرورية لتوفير قوانين وأنظمة تخصها؛ لتحدد هذه الجرائم وأركانها وعقوباتها. واعتمدت الدراسة على المنهج الوصفي التحليل المضمون ومناقشته والمنهج التأصيلي، وذلك اعتماداً على النظام السعودي والاجتهادات الفقهية والقانونية من خلال آراء الفقهاء والشرح. وتوصلت الدراسة إلى أن النظام مكافحة جرائم المعلوماتية حدد بشكل واضح مصطلحاته وأهدافه وعقوباته. كما يتناول النظام بالتفصيل عدداً من الجرائم المعلوماتية والأفعال غير المشروعة ويقسمها إلى مجموعات تحتوي كل مجموعة على عدد من الجرائم والعقوبات التي تخصها لتحقيق الأهداف التي وضع من أجلها. وقد أوصت الدراسة بضرورة توحيد الجهود الدولية ولاسيما الخليجية في مكافحة الجرائم المعلوماتية ، وبتشكيل لجان دائمة يكون مهمتها متابعة التطور التقني والمعلوماتي من أجل تطوير الأنظمة والقوانين التي تحمي الفرد والمجتمع من الجرائم المعلوماتية.

ثانياً: الدراسات الأجنبية:

- **دراسة (Almrezeq, Alserhani and Humayun, 2021) بعنوان " Exploratory Study to Measure Awareness of Cybercrime in Saudi Arabia "** تهدف الدراسة إلى قياس الوعي بالأمن السيبراني والجرائم المعلوماتية في المملكة العربية السعودية لطلاب جامعة الجوف. حيث أكدت أن المملكة العربية السعودية تركز على تعزيز نظام مكافحة الجرائم المعلوماتية وأنظمة الأمن السيبراني. وأشارت نتائجها أنه على الرغم من وجود زيادة في الوعي بالأمن السيبراني من قبل مجتمع الدراسة إلا أن هناك حاجة ملحة لفهم الأمن السيبراني والجرائم المعلوماتية من خلال التدريب والتعليم. كما أظهرت أن معظم الطلاب الذين تعرضوا للجرائم الإلكترونية لم يتعاملوا معها وفق القوانين والتشريعات المحلية في المملكة العربية السعودية ولم تكن

لديهم المعرفة بها، لذلك من الضرورة تسليط الضوء على هذه القوانين وتقويتها ونشرها. وزيادة برامج التوعية والإثراء بجرائم الإنترنت وكيفية التعامل معها وفق التشريعات المحلية لسد هذه الفجوة.

- دراسة (Alghamdi,2020) بعنوان " A Strategic Vision to Reduce Cybercrime to Enhance Cyber Security" سعت الدراسة إلى تطوير رؤية استراتيجية لمكافحة الجرائم الإلكترونية لتعزيز الأمن السيبراني في المملكة العربية السعودية، من خلال التعرف على طبيعة وأنواع الجرائم الإلكترونية وأبعاد الأمن السيبراني، ودور مكافحة الجرائم الإلكترونية في تعزيز الأمن السيبراني، باستخدام الاستبيان كأداة لجمع البيانات، وتوصلت الدراسة إلى عرض أبعاد الرؤية الاستراتيجية التطويرية لمكافحة الجرائم الالكترونية لتعزيز الأمن البشري في المملكة العربية السعودية. وقد أوصت الدراسة بضرورة توعية المجتمع السعودي (أفراداً ومؤسسات) بسبل الحماية من الجرائم الالكترونية، وإنشاء وحدة أمنية خاصة بوزارة الداخلية تختص بمكافحة الجرائم الالكترونية.
- دراسة (Alabdulatif, 2018) بعنوان " CYBERCRIME AND ANALYSIS OF LAWS IN KINGDOME OF SAUDI ARABIA" تهدف هذه الدراسة إلى تسليط الضوء على القوانين القائمة لمكافحة الجرائم الإلكترونية، ويتم إجراءها بناءً على المنهج التحليلي النقدي. وأظهرت الدراسة أن معظم الأفراد لديهم معرفة بالجرائم الإلكترونية، ولكن القليل منهم على دراية بتشريعات وقوانين المملكة العربية السعودية لمكافحة هذه الجرائم. لذلك أوصت الدراسة بالوعي بالقوانين القائمة في المجتمع السعودي، حيث إن إدراك القوانين الحالية سيساعد في تقليل معدل الجرائم الإلكترونية. أيضاً العمل على نشر القضايا الجرائم الإلكترونية سيزيد من الوعي بالقوانين القائمة وكيفية معالجتها.
- دراسة (Zayid and Farah, 2017) بعنوان " A Study on Cybercrime Awareness Test in Saudi Arabia – Alnamas Region"- هدفت الدراسة لإجراء اختبار وتقييم مخاطر الجرائم الإلكترونية الحالية والوعي في منطقة النماص، واستهدفت الدراسة مجموعة من المستخدمين على دراية كبيرة باستخدام تطبيقات وخدمات التكنولوجيا الحديثة. وأظهرت الدراسة أن الأسباب الكامنة وراء الجرائم الإلكترونية هي الجنسية ، والمالية ، والسياسية ، والثقافية ، والشهرة. ولكن شبكة التواصل الاجتماعي هي البوابة الأكثر انتشارًا لحدوث الجريمة الإلكترونية بمعدل (69.6%). ويعد برنامج مكافحة الفيروسات هو الأداة الوحيدة المستخدمة كأسلوب لمكافحة الجرائم الإلكترونية بشكل عام. وتوصلت نتائجها أن الأسباب الأكثر انتشاراً وراء الجرائم الإلكترونية هي الجرائم الجنسية حيث سجلت أعلى معدل (57٪). كما لاحظت الدراسة وجود نقصاً في الوعي بمعرفة الجرائم الإلكترونية ومخاطرها، وهناك رغبة قوية للمجتمع في تلقي تدريب ودعم لمكافحة الجرائم الإلكترونية بمعدل (80.7٪).
- دراسة (Elnaim, 2013) بعنوان " Cyber Crime in Kingdom of Saudi Arabia: The Threat Today and the Expected Future" تهدف إلى تحليل الجرائم الإلكترونية في المملكة العربية السعودية وقانون مكافحة الجرائم المعلوماتية. وقد أظهرت الدراسة أن قوانين الإنترنت في المملكة صدرت منذ عام 2007، لكن عدم الوعي بها بين الشباب قد خلق اختلالًا محتملاً بين الاستخدام الآمن للإنترنت والضعف في مواجهة الجريمة المعلوماتية، كما أكدت الدراسة أن معظم الناس لديهم معرفة بالجرائم المعلوماتية، ولكن القليل منهم على دراية بالتشريعات المرتبطة بها لمكافحة هذه الجرائم. وبالتالي إن عدم وعيهم بالقانون يؤدي ذلك إلى تزايد الجرائم الإلكترونية في جميع أنحاء المملكة العربية السعودية، وتشكل الحماية من التهديدات الإلكترونية تحديًا إداريًا مستمرًا للمؤسسات في البلاد.
-

العدد أربعون
تاريخ الإصدار: 2 – شباط – 2022 م
www.ajsp.net
ISSN: 2663-5798

ثالثاً: التعقيب على الدراسات السابقة

من خلال استعراض الدراسات السابقة في الإنتاج الفكري العربي والأجنبي؛ اتضح ان هناك مجموعة من النقاط التي تم اتفاق عليها في ادبيات الموضوع منها دراسة (عبدالرزاق، 2021) ودراسة (الخطيب، 2019) على بيان موقف التشريع السعودي اتجاه جرائم تقنية المعلومات. كما يتضح بأن بقية الدراسات السابقة اتفقت على أهمية توعية أفراد المجتمع بالجرائم المعلوماتية وأنظمة مكافحتها وما تنتج عنها من فوائد تساعد على تحقيق الأمن المعلوماتي، هذا وتتفق الدراسة الحالية مع الدراسات السابقة في الأهمية البالغة على تسليط الضوء على التوعية بقوانين وتشريعات نظام مكافحة الجرائم المعلوماتية السعودي للمساعدة على تقليل معدل الجرائم المعلوماتية، وأكد على ذلك (Elnaim, 2013) إن عدم الوعي بالقانون يؤدي ذلك إلى تزايد الجرائم الإلكترونية في جميع أنحاء المملكة العربية السعودية.

وتتميز الدراسة الحالية عن الدراسات السابقة في كونها ركزت على تناول مستوى وعي طلاب وطالبات الدراسات العليا بكلية الآداب والعلوم الانسانية في جامعة الملك عبدالعزيز بجدة بنظام مكافحة الجرائم المعلوماتية السعودي في ظل التحول الرقمي ضمن رؤية 2030، ومدى معرفتهم بأدوات الإبلاغ عن الجرائم المعلوماتية في السعودية، بالإضافة تطرقت الدراسة إلى رصد أسباب ضعف الوعي بنظام مكافحة جرائم المعلوماتية، والكشف عن أبرز طرق المكافحة والوقاية من الجرائم المعلوماتية حسب وجهة نظر أفراد عينة الدراسة.

حيث تختلف الدراسة في موضوعها ومجتمع الدراسة الذي لم يحظى سابقاً بدراسة ترصد مستوى وعيهم بالنظام السعودي. كما استفادت الدراسة الحالية من الدراسات السابقة في تصميم أداة الدراسة (الاستبانة)، ومعرفة أراء الباحثين ونظرياتهم واستنتاج توصياتهم والانطلاق منها بهذه الدراسة.

ثانياً: الإطار النظري

1 مفهوم الجريمة المعلوماتية

تعد الجريمة المعلوماتية موضوعاً واسعاً، فهي ظاهرة إجرامية يعاني منها المجتمع في الآونة الأخيرة من انتهاك للحقوق والخصوصية الالكترونية، حيث أصبح الحاسب الآلي بشكل عام وشبكة الانترنت بشكل خاص أدوات لارتكاب الجريمة المعلوماتية (بن عامر، 2021،ص803).

ولقد ظهرت العديد من المصطلحات والمسميات التي تُعبر عن الجرائم المعلوماتية نظراً لتعدد وتنوع أنماط صورها وهي (الجرائم الالكترونية، وجرائم تقنية المعلومات، وجرائم الانترنت).

كما تعددت التعريفات التي قدمتها الأدبيات حول مفهوم الجرائم المعلوماتية باعتبارها ظاهرة مستحدثة مازالت قيد الدراسة، نذكر أهمها:

ذهب (متولي، 2015، ص186) إلى أن الجريمة المعلوماتية هي "كل استخدام في صورة فعل أو امتناع غير مشروع للتقنية المعلوماتية ويهدف إلى الاعتداء على أي مصلحة مشروعة سواء أكانت مادية أو معنوية".

وقد أشار (الخطيب، 2019، ص113) بأنها" كل سلوك سلبي أو إيجابي يتم بموجبه الاعتداء على البرامج أو المعلومات أو الاستفادة منها بأية صورة كانت".

بينما ذكر (عمارة،2019، ص82) بأنها "نشاط غير مشروع موجه لنسخ أو الوصول إلى المعلومات المخزنة داخل الحاسوب، أو تغييرها، أو حذفها، أو الوصول إليها، أو التي تحول عن طريقه".

العدد أربعون
تاريخ الإصدار: 2 – شباط – 2022 م
www.ajsp.net
ISSN: 2663-5798

أما بالنسبة لنظام مكافحة جرائم المعلوماتية السعودي فقد نص الجريمة المعلوماتية في المادة الأولى بأنها "أي فعل يرتكب متضمناً استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام" (نص نظام مكافحة جرائم المعلوماتية، 2007).

ومن خلال ما سبق يتضح أن هناك اتفاق في معظم الجهود الرامية لوضع تعريف الجرائم المعلوماتية تمثلت في أنها توظيف التقنيات الرقمية بشكل سلبي لتبرير الاعتداء والقرصنة والوصول إلى المعلومات بدون وجه حق بهدف الحاق الضرر والاتلاف والتعدي على حقوق الآخرين.

وقد اعتمدت الدراسة على تبني التعريف الاجرائي للجريمة المعلوماتية على النحو الآتي: هي السلوك الغير مشروع في استخدام الشبكة المعلوماتية، ووسائل تقنية المعلومات لأغراض معينة أو الحاق الضرر بهم.

وبعد التعرف على المفاهيم المرتبطة بالجرائم المعلوماتية وسبل مكافحتها تحاول الدراسة أن تستعرض سمات وخصائص الجريمة المعلوماتية.

2 خصائص الجريمة المعلوماتية

تتسم الجرائم المعلوماتية بشكل عام بأنها جريمة عابرة للحدود ومستترة يصعب عادة اكتشافها؛ كما تتسم الجريمة المعلوماتية بمجموعة من الخصائص التي تميزها عن الجريمة التقليدية، أوضحتها دراسة (المقصودي، 2017؛ المطوع، 2021) تلخصها الدراسة على النحو الآتي:

1) **عابرة للحدود:** اذ أن الجريمة المعلوماتية بالظروف المكانية ولا الزمانية إنما تتجاوزها مستغلة في ذلك إمكانيات التقنيات الرقمية.
2) **جرائم ناعمة:** يقصد بها أنها لا تتطلب أي عنف في التلاعب بالبيانات والمعلومات من خلال نقلها أو حذفها...الخ؛ بل تعتمد على القدرة الذهنية في معرفة تقنيات الحاسب الآلي.
3) **صعبة الإثبات:** يصعب غالباً العثور على أثر مادي للجريمة المعلوماتية؛ لأنها جرائم لا تترك أثراً بعد ارتكابها، وذلك لسرعة وسهولة محو الدليل والتلاعب به.
4) **الإزالة:** يقصد أن الجريمة المعلوماتية لا تتطلب الإزالة، حيث يمكن أن يتم نسخها دون إزالتها.
5) **التوافر:** يقصد توفر المعلومات وتواجدها في كل وقت وعلى اختلاف الأماكن.
6) **المتعة:** يقصد أن الجرائم المعلوماتية تحمل العديد من الجوانب التسلية والاثارة والمتعة خلال ممارستها وارتكابها.
7) **الجاذبية:** تستهدف الجريمة المعلوماتية بشكل جاذب استغلال الأموال بطرق غير مشروعة.
8) **الاستدامة:** إمكانية استخدام المعدات والبرامج المسروقة لفترات زمنية ممتدة.
9) **إخفاء الجريمة:** تعد الجريمة المعلوماتية جريمة مخفية، وعلى الرغم من ذلك هناك إمكانية تسهم في التوقع بحدوثها وتخمين السيناريوهات المرتبطة بها للحماية أو التقليل من الآثار المترتبة عليها.
10) **سرعة التنفيذ:** يحسب للجريمة المعلوماتية سرعة تنفيذها، وذلك من خلال التطبيقات فائقة السرعة.
11) **التنفيذ عن بعد:** لا يتطلب في القيام بالجريمة المعلوماتية الوجود المادي أو الجسدي لوجود المجرم في ساحة الجريمة إذ أنها تتم بشكل افتراضي.

العدد أربعون
تاريخ الإصدار: 2 – شباط – 2022 م
www.ajsp.net
ISSN: 2663-5798

وبعد التطرق لسمات وخصائص الجرائم المعلوماتية يبرز سؤالاً وهو: ماهي أركان الجريمة المعلوماتية؟ ستجيب عنه الدراسة في السياق الآتي:

1. أركان الجريمة المعلوماتية:

تتمثل أركان الجريمة المعلوماتية على ثلاثة أركان رئيسة وهي كما على النحو الآتي:

- **أولاً: الركن المادي:** وينظر إليه أنه هيكل الجريمة إذ أنه يتمثل في الفعل الصادر على المرتكب لهذه الجريمة بهدف الاعتداء على المصالح العامة.
- **ثانياً: الركن المعنوي:** وهو الذي يمثل خلفية الشخص والنوايا المتوفرة لديه حيال العمل المصنف بالجريمة المعلوماتية بمعنى أنه يرتكبها وهو مدرك لعواقبها ودون اكراه.
- **ثالثاً: الركن القانوني:** وهو الذي يوظف التشريعات والقوانين لمحاسبة من يقوم بالجرائم المعلوماتية. (الربيعة، د.ت، ص4)

وتكاد تكون هذه الأركان هي الرئيسة المتداولة في أدبيات الموضوع، ولكن المجال الموضوعي حديثاً وقابلاً للزيادة أو النقصان في المستقبل، وقد تنوعت في صورها وأسباب حدوثها وكذلك في رصد الطرق المتنوعة لمكافحتها وهو ما سيتم عرضه في العرض اللاحق.

3 أنواع الجريمة المعلوماتية

تعددت الجرائم المعلوماتية لحداثتها، ولكن يمكن إجمالها بشكل عام إلى ثلاثة أنواع على النحو الآتي:

- الجرائم الموجهة ضد الافراد وتدور حول سرقة البيانات الشخصية والهوية وانتحال الشخصية والسطو على الاشتراكات او اختراق البريد الالكتروني بطرق غير شرعية والهدف الرئيس هو استغلال هوية الفرد في تيسير مهام القيام بالجرائم الكترونية واخفاء هوية المجرم الرئيس.
- الجرائم الموجهة ضد الملكية تتمثل في عمليات نقل واستخدام البرمجيات الخبيثة هي البرامج ذات الطبيعة الخدمية والتطبيقية بهدف الحاق الضرر ببرامج البنوك والشركات واتلاف الأجهزة والممتلكات الخاصة.
- الجرائم الموجهة ضد الجهات الحكومية هي التي تتمثل في مهاجمة مواقع الحكومات الرسمية وتستهدف أنظمة شبكاتها على كافة المستويات المحلية والدولية بغرض استهداف البنية التحتية ومهاجمة الشبكات الحاسوبية منها على سبيل المثال لا الحصر الهجمات الإرهابية. (الدوسري،2021)

4 أسباب الجريمة المعلوماتية

تناول الإنتاج الفكري العديد من الأسباب التي يمكن أن تكون سبباً في حدوث الجريمة المعلوماتية وأكدت الآراء أن هذه الأسباب متغيرة ومتفاوتة يحكمها العديد من العوامل مثل: نوع الجريمة، نوع الجاني، الغرض المستهدف. ويمكن إجمالها فيما يأتي:

أولاً: أسباب الجريمة المعلوماتية على المستوى الشخصي

1- الحاجة إلى التقدير والبحث المستمر عنه، ويتجسد ذلك السبب بشكل أكبر لدى الفئة العمرية صغيرة السن وقد تختفي تدريجاً مع التقدم في العمر.

2- الشعور بالإحباط والضغوط الحياتية التي تكون سبباً فيتعرض الفرد لمجموعة من المواقف السلبية مثل فقدان الوظيفة أو الخصم من الرواتب أو عدم الترقية المستحقة... الخ.

3- الفراغ وغياب المراقبة وفقدان التوجيه المستمر في البيئة المحيطة بالفرد.

ثانياً: أسباب الجريمة المعلوماتية على المستوى المجتمعي

1. الرغبة لتحقيق الثراء السريع دون الالتفات لسلك الطريق الصحيح للوصول إلى ذلك، مما يؤدي إلى انتشار سلوكيات غير مقبولة.
2. البطالة: يعد العمل مصدراً لأمان الفرد والمجتمع إذ أن وجود مصدر دخل مادي يؤدي للشعور بالاستقرار والعكس صحيح، كما وأن عدم الاستقراء الوظيفي والمادي قد يتسببا في توجه المجتمع نحو الجرائم المعلوماتية.
3. الافتقار إلى التشريعات والقوانين المنظمة أو عدم معرفة المجتمع بها.

ثالثاً : أسباب الجريمة المعلوماتية على المستوى الكوني

1) العولمة والتي ساهمت في تقليص الحواجز الجغرافية والزمنية وجعلت العالم قرية كونية صغيرة مما ساهم في نشوء الجريمة المعلوماتية المتخطية والعابرة للحدود.

2) التحول الرقمي واستخدام التطبيقات الرقمية وبروز مفهوم المجتمعات الافتراضية ساهم هو الآخر في إعطاء مساحة للجريمة المعلوماتية.

5 طرق مكافحة الجرائم المعلوماتية

وبعد التعرف على مفهوم الجرائم المعلوماتية وخصائصها وأركانها وأنواعها والأسباب المؤدية لحدوثها لابد من التطرق إلى معرفة طرق مكافحتها والتصدي لها، كما ناقشت الآراء المطروحة في أدبيات الموضوع طرق وأساليب متعددة للتصدي من الجرائم المعلوماتية والآثار المترتبة عليها وهي كما على النحو الآتي: (الربيعة، د.ت، ص13)

1- زيادة الوعي بالجرائم المعلوماتية والتثقيف بمخاطرها، وتوجيه الأفراد بضرورة المحافظة على معلوماتهم الخاصة وحفظ تلك الخصوصية بكلمات مرور قوية بما يتعلق بمسائلهم الشخصية مثل أرقامهم الوظيفية والحسابات البنكية والبطاقات الائتمانية.
2- سن التشريعات والقوانين التي تتسم بالمرونة والحداثة ومواكبة التطورات التقنية لحماية الفرد والمجتمع من الجرائم المعلوماتية.
3- تخصيص مؤسسات خدمية في المجتمع يسهل الوصول إليها أرقام تواصل سهلة للإبلاغ عن الجرائم المعلوماتية.
4- توظيف التقنيات الرقمية للمساهمة في كشف هوية منفذي الجريمة المعلوماتية.
5- إصدار السياسات المنظمة لعقوبات تطبق على منفذي الجرائم المعلوماتية على المستويين الدولي والمحلي.

وبعد الاستعراض الشامل لمفهوم الجريمة المعلوماتية وخصائصها وأركانها وأنواعها وأسبابها وطرق مكافحتها، سيتم التركيز على نظام مكافحة الجرائم المعلوماتية في المملكة العربية السعودية – مجال الدراسة –.

6 نبذة عن نظام مكافحة الجرائم المعلوماتية في المملكة العربية السعودية

شهدت المملكة العربية السعودية تطوراً ملحوظاً في مجال التحول الرقمي وحققت نقلة نوعية في استخدام التقنيات الرقمية بالمجتمع، وتعد من أوائل الدول العربية في إصدار نظاماً لمكافحة الجرائم المعلوماتية في هذا المجال وذلك بموجب المرسوم الملكي رقم م/17 وتاريخ 1428/3/8 هـ بناءً على قرار مجلس الوزراء رقم 79 وتاريخ 1428/3/7 هـ. وقد شمل النظام على ستة عشر مادة أورد المنظم في هذا النظام التعريفات بالألفاظ والعبارات التي تخص النظام؛ وأهداف النظام؛ والجرائم المعلوماتية وعقوبات مرتكبيها إضافة إلى أحكام مشددات العقوبة والاعفاء عنها، وأحكام الشروع في الجريمة المعلوماتية والاشتراك بها، والعقوبة التكميلية لها؛ وأخيراً الجهات ذات العلاقة في التحقيق فيها.

7 أهداف نظام مكافحة الجرائم المعلوماتية في المملكة العربية السعودية

يحدد النظام مجموعة من الأهداف التي يسعى لتحقيقها من خلال الأحكام والعقوبات المذكورة فيه، حيث نصت المادة الثانية من نظام مكافحة جرائم المعلوماتية على أن هذا النظام يسعى إلى تقليص حدوث الجرائم المعلوماتية وذلك بتوضيح تلك الجرائم وتحديد العقوبات المفروضة لها حسب أنواعها. كما ذكر النظام مجموعة من الأهداف التابعة لها يفسرها (اليحيى، 2013، ص285) فيما يأتي:

1) الوصول إلى الأمن المعلوماتي وتحقيقها

يتضمن هذا الهدف كافة القضايا الأمنية التي يتناولها النظام ويعزز فكرة تقليص الجرائم والبعد عن التحريض على ارتكاب الجرائم المعلوماتية وتصوير سهولة إجراءاتها وحدوثها مثل الإرهاب والابتزاز والتجسس.

2) الحفاظ على الحقوق الناتجة عن الاستخدام القانوني للحاسبات والشبكات المعلوماتية

يركز هذا الهدف على الاستخدام القانوني للتقنية وتطبيقاتها مع المحافظة على الحقوق المادية والاجتماعية والملكية الفكرية.

3) حماية المصلحة العامة، والأخلاق، والآداب العامة

الحفاظ على كل ما يرتبط بالأخلاقيات والآداب العامة والقيم ومصلحة المجتمع. للوصول لتحقيق متطلبات هذا الهدف ركز النظام على ضرورة عدم التعارض مع الدين أو الآداب أو الأخلاق حيث يعاقب النظام على ذلك.

4) المحافظة على الاقتصاد الوطني وحمايته

تتطلب حماية الاقتصاد الوطني ضمان حماية الأموال العامة والخاصة.

1. نظام مكافحة الجرائم المعلوماتية السعودي: من منظور قانوني

حسمت المملكة العربية السعودية قضايا الجرائم المعلوماتية والعقوبات المرتبطة بها من خلال القانون الجنائي، والذي يستمد في المملكة العربية السعودية من الشريعة، وقد حقق تميزاً وشمولاً وتكاملاً في تغطية وتنظيم كافة الأمور الحياتية (الربيعة، د.ت، ص6-7).

2. نظام مكافحة الجرائم المعلوماتية السعودي: أبرز المصطلحات

وضح النظام أبرز المصطلحات المدرجة به ووضع لها تعريفات إجرائياً ووضح مفاهيمها لإزالة اللبس والغموض بشأنها ومنها ما يأتي:

- **الشخص:** هو أي فرد له صفة اعتبارية عامة أو خاصة.
- **النظام المعلوماتي:** حزمة من البرامج والأدوات التي تستخدم لمعالجة وإدارة البيانات منها الحاسبات الآلية.
- **الشبكة المعلوماتية:** تتنوع بالشبكات العامة والخاصة والشبكة العالمية (الانترنت)، وتقوم في محورها على الربط بين أكثر من جهاز أو نظام معلوماتي بهدف الحصول على البيانات ومعالجتها وتبادلها.
- **البيانات:** هي مجموعة من الأرقام والرموز والمعلومات والرسائل والصور المعالجة رقمياً بواسطة الحاسب الآلي.
- **الدخول غير المشروع:** ويعني استخدام الفرد بشكل متعمد للمواقع الالكترونية والأنظمة المعلوماتية والشبكات بشكل غير مصرح له.

3. نظام مكافحة الجرائم المعلوماتية السعودي: أنواع الجرائم المعلوماتية

بعد التعرف على أبرز المصطلحات الواردة في نظام مكافحة الجرائم المعلوماتية السعودي، يتم تسليط الضوء على أنواع متعددة من الجرائم المعلوماتية حصرها النظام في الآتي: (نص نظام مكافحة الجرائم المعلوماتية، 2007)

1) التنصت:

صُنف التنصت بكافة أنماطه على أنه جريمة معلوماتية قائمة على محاولات متعددة الصور في اعتراض أو التقاط أو التجسس دون مبررات نظامية.

2) اختراق المواقع الالكترونية:

وتتمثل في محاولة الدخول للموقع الالكتروني والعبث في تصاميمه وإلحاق التلف به من خلال إضافات أو تعديلات أو تشويش على العنوان الالكتروني بشكل غير قانوني. ولا تقتصر على المواقع الالكترونية إنما تمتد لإلحاق الضرر بالشبكة المعلوماتية الانترنت بهدف تعطيلها أو إيقاف بعض الخدمات الالكترونية.

3) الاستخدام الغير مقنن للهواتف المحمولة:

وهو عبارة عن توظيف الهواتف المحمولة بما يلحق الضرر سواء باستخدام الكاميرا أو بدونها وقد تسبب هذه النوعية من الجرائم في إحداث العديد من المشاكل النفسية والاجتماعية على مستوى الفرد والجماعة.

4) الانتحال والاستيلاء:

تدور فكرة هذه الجريمة حول التخفي خلف أسماء وهمية وصفات غير سليمة والتسبب في توقيع مجموعة من السندات لأغراض غير مشروعة.

5) التعدي على البنوك:

تدور في محورها حول تيسير الوصول غير المشروع للبيانات البنكية وبيانات البطاقات الائتمانية والخدمات البنكية المختلفة بهدف التعدي.

6) التشهير:

تتمثل في محاولة إبراز الجوانب السلبية في الأشخاص أو الكيانات من خلال توظيف التقنيات الرقمية بهدف إلحاق الضرر بهم.

7) التهديد والابتزاز:

وهما من الطرق غير المشروعة إذ أنهما ينتهجان أسلوب الضغط والتخويف من خلال المجرم بما يمتلك من معلومات، أو صور، أو أخبار مغلوطة وملفقة، أو صحيحة ويحاول أن يستخدمها لجني الأموال غير المشروعة من قبل المجني عليه.

8) المساس بالنظام العام، أو القيم الدينية، أو الآداب العامة ، أو حرمة الحياة الخاصة:

نصت الفقرة الأولى من المادة السادسة من النظام على أن جريمة "إنتاج ما من شأنه المساس بالنظام العام ، أو القيم الدينية، أو الآداب العامة ، أو حرمة الحياة الخاصة، أو إعداده ، أو إرساله، أو تخزينه عن طريق الشبكة المعلوماتية ، أو أحد أجهزة الحاسب الآلي".

9) الاتجار بالبشر والاتجار بالمخدرات والجرائم المعلوماتية الأخلاقية:

وقد نصت المادة السادسة من النظام على الجرائم المعلوماتية الآتية:

- "إنشاء موقع على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي أو نشره للإتجار في الجنس البشري أو تسهيل التعامل به".
- "إنشاء المواد والبيانات المتعلقة بالشبكات الإباحية، أو أنشطة الميسر المخلة بالآداب العامة أو نشرها أو ترويجها".
- " إنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره، للاتجار بالمخدرات، أو المؤثرات العقلية، أو ترويجها، أو طرق تعاطيها، أو تسهيل التعامل بها".

10) جرائم أمن المعلومات:

وقد نصت المادة السابعة من النظام على الجرائم المعلوماتية الآتية:

- "إنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية ، أو أحد أجهزة الحاسب الآلي أو نشره؛ لتسهيل الاتصال بقيادات تلك المنظمات، أو أي من أعضائها، أو ترويج أفكارها، أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرات، أو أي أداة تستخدم في الأعمال الإرهابية".
- "الدخول غير المشروع إلى موقع إلكتروني ، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية ، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني".

العدد أربعون
تاريخ الإصدار: 2 – شباط – 2022 م
www.ajsp.net
ISSN: 2663-5798

4. العقوبات المترتبة على المشاركة في الجرائم المعلوماتية وتنفيذها

بعد استعراض الجرائم المعلوماتية المدرجة في نظام مكافحة الجرائم المعلوماتية السعودي، نجد أن النظام رسم إطاراً تنظيمياً للعقوبات الرادعة للأطراف المشاركة في الجريمة المعلوماتية.

ونصت المادة التاسعة من نظام مكافحة جرائم المعلوماتية على ذلك وهي " يعاقب كل من حرَّض غيره، أو ساعده، أو اتفق معه على ارتكاب أيٍّ من الجرائم المنصوص عليها في هذا النظام ؛ إذا وقعت الجريمة بناء على هذا التحريض، أو المساعدة، أو الاتفاق، بما لا يتجاوز الحد الأعلى للعقوبة المقررة لها ، ويعاقب بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة لها إذا لم تقع الجريمة الأصلية".

كما نصّت المادة العاشرة من نظام مكافحة جرائم المعلوماتية بأن "يعاقب كل من شرع في القيام بأي من الجرائم المنصوص عليها في هذا النظام بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة". (نص نظام مكافحة الجرائم المعلوماتية، 2007)

5. أدوات الإبلاغ عن الجرائم المعلوماتية في المملكة العربية السعودية

نصت المادة الرابعة عشرة من نظام مكافحة جرائم المعلوماتية بأن "تتولى هيئة الاتصالات وتقنية المعلومات وفقًا لاختصاصها تقديم الدعم والمساندة الفنية للجهات الأمنية المختصة خلال مراحل ضبط هذه الجرائم والتحقيق فيها وأثناء المحاكمة". فقد ساندت (هيئة الاتصالات وتقنية المعلومات، 2017) بالتعريف بأبرز أدوات الإبلاغ عن الجرائم المعلوماتية وهي كما على النحو الآتي:

1- **مركز الشرطة:** يتم البلاغ من خلال أقرب مركز للشرطة.

2- **البريد الإلكتروني:** يتم إرسال البلاغ إلى البريد الالكتروني الخاص بالجرائم المعلوماتية وهو كالآتي: (info.cybercrime@moisp.gov.sa).

3- **الاتصال على الرقم 989.**

4- **بوابة وزارة الداخلية (أبشر):**

وهي خدمة إلكترونية تقدمها مديرية الأمن العام تمكن المستفيد من الإبلاغ عن الجرائم الإلكترونية بمختلف أنواعها. حيث يتم الإبلاغ عن الجريمة المعلوماتية بشكل إلكتروني وبشكل سري وتتم متابعتها من قبل مختصين ويمكن رفع البلاغ عن الجريمة المعلوماتية عبر (أبشر) **من خلال الخطوات الآتية:**

الدخول إلى بوابة وزارة الداخلية (أبشر)، ثم الدخول إلى خدمات الأمن العام، ثم اختيار بلاغ الجرائم الإلكترونية، بعد ذلك اختيار نوع البلاغ والقيام بتعبئة الحقول المطلوبة، وأخيراً إرسال البلاغ وسيتم تزويد الفرد برقم مرجعي للبلاغ (المنصة الوطنية الموحدة، 2021).

5- **تطبيق كلنا أمن:**

وهي خدمة تتيح للمواطن والمقيم تقديم البلاغات الأمنية والجنائية، وذلك إلكترونياً من خلال تطبيق (كلنا أمن). حيث يتم الإبلاغ عن الجريمة المعلوماتية بشكل إلكتروني وسري وتتم متابعتها من قبل مختصين ويمكن رفع البلاغ عبر تطبيق كلنا أمن على الأجهزة الذكية التابع للأمن العام. **وتتم من خلال الخطوات الآتية:**

القيام بتحميل تطبيق (كلنا أمن) من المتجر، ثم القيام بفتح التطبيق وتقديم البلاغ، وبعد ذلك سيتم الاشعار باستقبال البلاغ والعمل عليه من قبل الجهات المختصة (المنصة الوطنية الموحدة، د.ت).

ثالثاً: الإطار التطبيقي

i. إجراءات الدراسة وأداتها

اتبعت الدراسة أداة الاستبانة لجمع المعلومات والبيانات اللازمة، لمناسبتها للمنهج المتبع في الدراسة، والأكثر ملائمة لتحقيق أهدافها والإجابة على تساؤلاتها. وقد تم الاعتماد عند إعداد الاستبانة بالاطلاع على الأدبيات والدراسات السابقة المتعلقة بموضوع الدراسة، والأخذ بآراء المحكمين الذين عرضت عليهم الاستبانة في صورتها المبدئية بما يتناسب مع أهداف الدراسة؛ **وبناء على ذلك تم تصميم أداة الاستبانة وقد تكونت من قسمين وهما كالآتي:**

أ- **القسم الأول:** يشتمل الجزء الأول على البيانات الأولية لأفراد عينة الدراسة كما على النحو الآتي:

(النوع، المرحلة الدراسية، التخصص العلمي).

ب- **القسم الثاني:** يشتمل الجزء الثاني على محاور الاستبانة وهي كما على النحو الآتي:

1- المحور الأول: الوعي بالجرائم المعلوماتية المذكورة بنظام مكافحة الجرائم المعلوماتية السعودي، واحتوى على (14) عبارة.

2- المحور الثاني: من وجهة نظرك ماهي أسباب ضعف الوعي بنظام مكافحة جرائم المعلوماتية السعودي؟، واحتوى على (5) عبارات.

3- المحور الثالث: من وجهة نظرك ماهي أبرز الطرق للمكافحة والوقاية من الجرائم المعلوماتية في ظل التحول الرقمي تماشياً مع رؤية 2030؟، واحتوى على (9) عبارات.

4- المحور الرابع: هل لديك معرفة بأنه يمكنك الإبلاغ عن الجرائم المعلوماتية من خلال أحد الأدوات التالية؟، واحتوى على (5) عبارات.

وقد تم توزيع الاستبانة على مجتمع الدراسة البالغ عددهم (1829) طالباً وطالبة، وتم أخذ عينة عشوائية ممثلة لمجتمع الدراسة بلغ عددها (317) طالباً وطالبة، وذلك وفق ما حدده جدول كرجسي ومورغان (Krejcie & Morgan, 1970)، وبذلك يكون عدد الاستبانات التي تم تحليلها (317) استبانة صالحة للتحليل الإحصائي.

- **صدق أداة الدراسة:**

أ- صدق الاتساق الظاهري لأداة الدراسة:

للتحقق من الصدق الظاهري للاستبانة تم عرضها على مجموعة من المحكمين المتخصصين من أعضاء هيئة التدريس في قسم علم المعلومات بجامعة الملك عبدالعزيز، وفي ضوء أراءهم ومقترحاتهم تم تصميم أداة الدراسة.

ب- صدق الاتساق الداخلي لأداة الدراسة:

العدد أربعون
تاريخ الإصدار: 2 – شباط – 2022 م
www.ajsp.net
ISSN: 2663-5798

بعد التأكد من الصدق الظاهري لأداة الدراسة تم حساب معامل الارتباط بيرسون لمعرفة الصدق الداخلي للاستبانة، وذلك عن طريق حساب معامل الارتباط بين درجة كل عبارة من عبارات الاستبانة بالدرجة الكلية للمحور الذي تنتمي إلية العبارة، كما هو موضح في الجداول الآتية رقم (1) – (2) – (3) – (4).

جدول رقم (1) معاملات ارتباط بيرسون لعبارات المحور الأول (الوعي بالجرائم المعلوماتية المذكورة بنظام مكافحة الجرائم المعلوماتية السعودي)

رقم العبارة	معامل الارتباط
1	**0.554
2	**0.645
3	**0.514
4	**0.539
5	**0.526
6	**0.478
7	**0.417
8	**0.432
9	**0.623
10	**0.628
11	**0.537
12	**0.537
13	**0.459
14	**0.437

** دال عند مستوى الدلالة 0.01 فأقل

جدول رقم (2) معاملات ارتباط بيرسون لعبارات المحور الثاني (من وجهة نظرك ماهي أسباب ضعف الوعي بنظام مكافحة جرائم المعلوماتية السعودي؟)

رقم العبارة	معامل الارتباط
1	**0.553
2	**0.716
3	**0.686
4	**0.752
5	**0.735

** دال عند مستوى الدلالة 0.01 فأقل

جدول رقم (3) معاملات ارتباط بيرسون لعبارات المحور الثالث (من وجهة نظرك ماهي أبرز الطرق للمكافحة والوقاية من الجرائم المعلوماتية في ظل التحول الرقمي تماشياً مع رؤية 2030؟)

رقم العبارة	معامل الارتباط
1	**0.510
2	**0.682
3	**0.704
4	**0.661
5	**0.591
6	**0.721
7	**0.687
8	**0.671
9	**0.612

** دال عند مستوى الدلالة 0.01 فأقل

جدول رقم (4) معاملات ارتباط بيرسون لعبارات المحور الرابع (هل لديك معرفة بأنه يمكنك الإبلاغ عن الجرائم المعلوماتية من خلال أحد الأدوات التالية؟)

رقم العبارة	معامل الارتباط
1	**0.495
2	**0.559
3	**0.843
4	**0.838
5	**0.794

** دال عند مستوى الدلالة 0.01 فأقل

يتضح من الجداول السابقة رقم (1) – (2) – (3) – (4) ما يأتي:

أن قيم معامل ارتباط كل عبارة من العبارات مع المحور الذي تنتمي له موجبة ودالة إحصائياً عند مستوى الدلالة (0.01) فأقل، مما يدل على صدق الاتساق الداخلي بين عبارات المحور والدرجة الكلية للمحور، وتمتعها بدرجة صدق عالية صلاحيتها للتطبيق.

- **ثبات أداة الدراسة:**

لقياس مدى ثبات أداة الدراسة (الاستبانة) تم استخدام (معادلة ألفا كرونباخ) ((Cronbach's Alpha (α)) للتأكد من ثبات أداة الدراسة، والجدول رقم (5) يوضح معاملات ثبات أداة الدراسة.

جدول رقم (5) معامل ألفا كرونباخ لقياس ثبات أداة الدراسة

محاور وأبعاد الاستبانة	عدد العبارات	معامل ألفا كرونباخ
المحور الأول: الوعي بالجرائم المعلوماتية المذكورة بنظام مكافحة الجرائم المعلوماتية السعودي	14	0.78
المحور الثاني: من وجهة نظرك ماهي أسباب ضعف الوعي بنظام مكافحة جرائم المعلوماتية السعودي؟	5	0.73
المحور الثالث: من وجهة نظرك ماهي أبرز الطرق للمكافحة والوقاية من الجرائم المعلوماتية في ظل التحول الرقمي تماشياً مع رؤية 2030؟	9	0.80
المحور الرابع: هل لديك معرفة بأنه يمكنك الإبلاغ عن الجرائم المعلوماتية من خلال أحد الأدوات التالية؟	5	0.76
معامل الثبات الكلي للاستبانة	**33**	**0.70**

يتضح من الجدول رقم (5) ما يأتي:

أن معاملات ثبات ألفا كرونباخ كانت مرتفعة في جميع المحاور، وأن معامل الثبات العام قد بلغ (0.70)، وهذا يدل على أن الاستبانة تتمتع بدرجة عالية من الثبات يمكن الاعتماد عليها في التطبيق الميداني للدراسة.

- **أساليب المعالجة الإحصائية:**

لتحقيق أهداف الدراسة وتحليل بياناتها اتبعت الدراسة عدداً من الأساليب الإحصائية المناسبة باستخدام الحزم الإحصائية للعلوم الاجتماعية، والتي يرمز لها اختصاراً بالرمز (SPSS)، وذلك بعد أن تم ترميز البيانات وإدخالها إلى الحاسب الآلي، ثم استخرجت النتائج وفقاً للأساليب الإحصائية الآتية:

1. **التكرارات والنسب المئوية؛** لوصف خصائص أفراد عينة الدراسة.
2. **المتوسطات الحسابية والانحراف المعياري:** لمعرفة اتجاهات إجابات أفراد عينة الدراسة لكل عبارة من عبارات الاستبانة، إلى جانب المحاور الرئيسية.

3. **معامل ارتباط بيرسون (Pearson)**؛ لقياس صدق الاتساق الداخلي بين عبارات كل محور تنتمي إليه عبارات هذا المحور.
4. **معامل الثبات ألفا كرونباخ ((Cronbach's Alpha(α))**؛ لحساب معامل ثبات أداة الدراسة.

- **معيار الحكم على نتائج الدراسة:**

لتسهيل تفسير النتائج تم اتباع الأسلوب الآتي لتحديد مستوى الإجابة على بدائل المقياس، وذلك بإعطاء وزن للبدائل: (مدرك = 3، مدرك إلى حد ما = 2، غير مدرك =1)، كما يتضح من الجدول رقم (6)، ثم صنفت تلك الإجابات إلى ثلاثة مستويات متساوية المدى عن طريق المعادلة الآتية:

طول الفئة = (أكبر قيمة–أقل قيمة) ÷ عدد بدائل المقياس = (3–1) ÷ 3= (0.66)

جدول رقم (6) درجات فئات معيار نتائج الدراسة وحدودها وفقًا لمقياس ليكرت الثلاثي

الدرجة	معيار الحكم على النتائج	فئة المتوسط	
		من	إلى
5	**غير مدرك**	1.00	1.67
2	**مدرك إلى حد ما**	1.67	2.33
1	**مدرك**	2.34	3.00

وكذلك لتسهيل تفسير النتائج تم اتباع الأسلوب الآتي لتحديد مستوى الإجابة على بدائل المقياس، وذلك إعطاء وزن للبدائل: (أقل أثراً = 5، أثر ضعيف = 4، أثر متوسط = 3، مؤثر = 2، أكثر أثراً=1)، كما يتضح من الجدول رقم (7)، ثم صنفت تلك الإجابات إلى خمس مستويات متساوية المدى عن طريق المعادلة الآتية:

طول الفئة = (أكبر قيمة–أقل قيمة) ÷ عدد بدائل المقياس = (5–1) ÷ 5= (0.80)

وللحصول على مدى المتوسطات التالية لكل وصف أو بديل.

جدول رقم (7) درجات فئات معيار نتائج الدراسة وحدودها وفقًا لمقياس ليكرت الخماسي

الدرجة	معيار الحكم على النتائج	فئة المتوسط	
		من	إلى
1	أكثر أثراً (مؤثر جداً)	1	1.80
2	مؤثر	1.81	2.60
3	أثر متوسط	2.61	3.40
4	أثر ضعيف	3.41	4.20

العدد أربعون
تاريخ الإصدار: 2 – شباط – 2022 م
www.ajsp.net
ISSN: 2663-5798

الدرجة	معيار الحكم على النتائج	فئة المتوسط	
		من	إلى
5	أقل أثراً (أثر ضعيف جداً)	4.21	5

2. عرض نتائج الدراسة ومناقشتها

- أولاً: وصف خصائص عينة الدراسة:

جدول رقم (8) توزيع أفراد عينة الدراسة وفقاً لمتغير النوع

النوع	التكرار	النسبة
ذكر	110	%34.7
أنثى	207	%65.3
المجموع	**317**	**٪100**

يتضح من الجدول رقم (8) ما يأتي:

أن (207) من أفراد عينة الدراسة يمثلون ما نسبته 65.3٪ من إجمالي أفراد عينة الدراسة إناث وهن الفئة الأكثر من أفراد عينة الدراسة، كما أن (110) منهم يمثلون ما نسبته 34.7٪ من إجمالي أفراد عينة الدراسة ذكور.

شكل بياني رقم (1) توزيع أفراد عينة الدراسة وفقاً لمتغير النوع

العدد أربعون
تاريخ الإصدار: 2 – شباط – 2022 م
www.ajsp.net
ISSN: 2663-5798

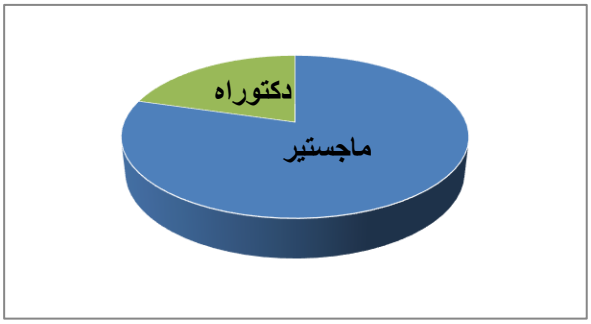
جدول رقم (9) توزيع أفراد عينة الدراسة وفقاً لمتغير المرحلة الدراسية

المرحلة الدراسية	التكرار	النسبة
ماجستير	252	%79.5
دكتوراه	65	%20.5
المجموع	**317**	**٪100**

يتضح من الجدول رقم (9) ما يأتي:

أن (252) من أفراد عينة الدراسة يمثلون ما نسبته 79.5٪ من إجمالي أفراد عينة الدراسة بمرحلة الماجستير وهم الفئة الأكثر من أفراد عينة الدراسة، كما أن (65) منهم يمثلون ما نسبته 20.5٪ من إجمالي أفراد عينة الدراسة بمرحلة الدكتوراه.

شكل بياني رقم (2) توزيع أفراد عينة الدراسة وفقاً لمتغير المرحلة الدراسية



جدول رقم (10) توزيع أفراد عينة الدراسة وفقاً لمتغير التخصص العلمي

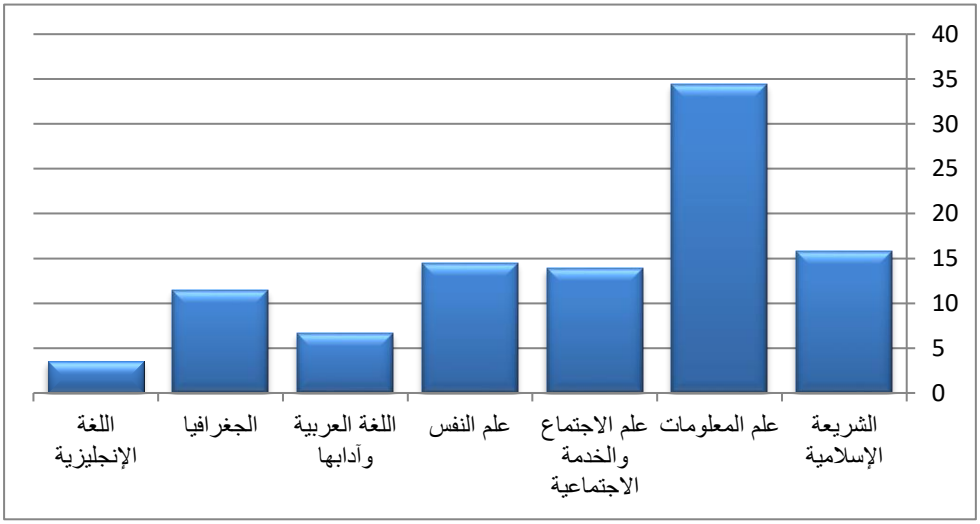
التخصص العلمي	التكرار	النسبة
الشريعة والدراسات الإسلامية	50	%15.8
علم المعلومات	109	%34.4
علم الاجتماع والخدمة الاجتماعية	44	%13.9
علم النفس	46	%14.5
اللغة العربية وآدابها	21	%6.6
الجغرافيا	36	%11.4
اللغة الإنجليزية	11	%3.5
المجموع	**317**	**٪100**

العدد أربعون
تاريخ الإصدار: 2 – شباط – 2022 م
www.ajsp.net
ISSN: 2663-5798

يتضح من الجدول رقم (10) ما يأتي:

أن (109) من أفراد عينة الدراسة يمثلون ما نسبته 34.4٪ من إجمالي أفراد عينة الدراسة تخصصهم علم معلومات وهم الفئة الأكثر من أفراد عينة الدراسة، بينما (50) منهم يمثلون ما نسبته 15.8٪ من إجمالي أفراد عينة الدراسة تخصصهم شريعة إسلامية، في حين أن (46) منهم يمثلون ما نسبته 14.5٪ من إجمالي أفراد عينة الدراسة تخصصهم علم نفس، مقابل (44) منهم يمثلون ما نسبته 13.9٪ من إجمالي أفراد عينة الدراسة تخصصهم علم اجتماع وخدمة اجتماعية، كما أن (36) منهم يمثلون ما نسبته 11.4٪ من إجمالي أفراد عينة الدراسة تخصصهم جغرافيا، وأن (21) منهم يمثلون ما نسبته 6.6٪ من إجمالي أفراد عينة الدراسة تخصصهم اللغة العربية وآدابها، و(11) منهم يمثلون ما نسبته 3.5٪ من إجمالي أفراد عينة الدراسة تخصصهم اللغة الإنجليزية.

شكل بياني رقم (3) توزيع أفراد عينة الدراسة وفقاً لمتغير التخصص العلمي



- **ثانياً: النتائج المتعلقة بتساؤلات الدراسة**

❖ **التساؤل الأول: ما مدى الوعي بالجرائم المعلوماتية المذكورة بنظام مكافحة الجرائم المعلوماتية السعودي لدى طلاب وطالبات الدراسات العليا بكلية الآداب والعلوم الإنسانية في جامعة الملك عبدالعزيز؟**

للتعرف على مدى الوعي بالجرائم المعلوماتية المذكورة بنظام مكافحة الجرائم المعلوماتية السعودي تم حساب المتوسطات الحسابية، والانحرافات المعيارية، والترتيب لإجابات أفراد عينة الدراسة على المحور الأول: الوعي بالجرائم المعلوماتية المذكورة بنظام مكافحة الجرائم المعلوماتية السعودي، وجاءت النتائج كما يوضحها الجدول الآتي:

AJSP
المجلة العربية للنشر العلمي
العدد أربعون
تاريخ الإصدار: 2 – شباط – 2022 م
www.ajsp.net
ISSN: 2663-5798

جدول رقم (11) إجابات أفراد عينة الدراسة على المحور الأول: مدى الوعي بالجرائم المعلوماتية المذكورة بنظام مكافحة الجرائم المعلوماتية السعودي

رقم العبارة	العبارة	التكرار	درجة الاستجابة			المتوسط الحسابي	الانحراف المعياري	الترتيب
		النسبة	مدرك	مدرك إلى حد ما	غير مدرك			
1	أدرك أن نظام مكافحة جرائم المعلوماتية يعاقب على التنصت على المواد المرسلة عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي.	ك	219	47	51	2.53	0.757	13
		٪	69.1	14.8	16.1			
2	يعاقب نظام مكافحة جرائم المعلوماتية من تسبب في إيقاف الشبكة المعلوماتية أو تعطيلها، أو مسح البرامج والبيانات المستخدمة فيها والتلاعب بها.	ك	204	43	70	2.42	0.829	14
		٪	64.4	13.6	22.1			
3	لا يحق لي الدخول الغير المشروع إلى الشبكة الالكترونية بهدف تهديد شخص أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه.	ك	291	24	2	2.91	0.306	2
		٪	91.8	7.6	0.6			
4	لا يحق لي الدخول الغير المشروع إلى أي موقع الكتروني دون إذن أو اختراقه.	ك	233	58	26	2.65	0.626	12
		٪	73.5	18.3	8.2			
5	لا يحق لي الدخول الغير المشروع لإلغاء بيانات خاصة أو التلاعب بها أو إعادة نشرها.	ك	278	26	13	2.84	0.469	8
		٪	87.7	8.2	4.1			
6	لا يحق لي الدخول الغير مشروع إلى موقع الكتروني أو نظام معلوماتي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني.	ك	302	15	0	2.95	0.213	1
		٪	95.3	4.7	0			
7	أدرك أن المساس بالحياة الخاصة من خلال إساءة استخدام الهواتف المحمولة يعرضني للمسؤولية.	ك	290	25	2	2.91	0.310	3
		٪	91.5	7.9	0.6			

AJSP
المجلة العربية للنشر العلمي
العدد أربعون
تاريخ الإصدار: 2 – شباط – 2022 م
www.ajsp.net
ISSN: 2663-5798

رقم العبارة	العبارة	التكرار	درجة الاستجابة			المتوسط الحسابي	الانحراف المعياري	الترتيب
		النسبة	مدرك	مدرك إلى حد ما	غير مدرك			
8	أكون تحت طائلة المسؤولية إذا قمت بالتشهير بالآخرين وإلحاق الضرر بهم عبر وسائل تقنيات المعلومات.	ك	292	21	4	2.91	0.330	5
		٪	92.1	6.6	1.3			
9	الوصول غير المشروع إلى البيانات البنكية والخدمات البنكية المختلفة يعاقب عليه نظام مكافحة جرائم المعلوماتية.	ك	270	33	14	2.81	0.494	10
		٪	85.2	10.4	4.4			
10	أدرك أن إعاقة الوصول إلى الخدمات عبر الشبكة المعلوماتية أو تعطيلها يعرضني للمسؤولية.	ك	249	42	26	2.70	0.611	11
		٪	78.5	13.2	8.2			
11	أكون تحت طائلة المسؤولية عند إنتاج محتوى ماس بالنظام العام، أو القيم الدينية، أو الآداب العامة، وتخزينه على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي.	ك	282	27	8	2.86	0.410	6
		٪	89.0	8.5	2.5			
12	إنشاء وتداول البيانات المتعلقة بالشبكات الإباحية أو أنشطة الميسر المخلة بالآداب العامة يعاقب عليه نظام مكافحة جرائم المعلوماتية.	ك	283	16	18	2.84	0.501	9
		٪	89.3	5.0	5.7			
13	ينص النظام على منع نشر المواقع ذات الصلة بالمخدرات وترويجها والتسويق لها.	ك	282	22	13	2.85	0.460	7
		٪	89.0	6.9	4.1			
14	إنشاء أو نشر مواقع لمنظمات إرهابية على الشبكة المعلوماتية أو ترويج أفكارها وتمويلها يعاقب عليه نظام مكافحة جرائم المعلوماتية.	ك	293	21	3	2.91	0.312	4
		٪	92.4	6.6	0.9			
المتوسط الحسابي العام – الانحراف المعياري العام						2.79	0.257	

يتضح من الجدول رقم (11) ما يأتي:

أن هناك تجانس في موافقة أفراد عينة الدراسة على مدى الوعي بالجرائم المعلوماتية المذكورة بنظام مكافحة الجرائم المعلوماتية السعودي، حيث تراوحت متوسطات موافقتهم على مدى الوعي بالجرائم المعلوماتية المذكورة بنظام مكافحة الجرائم المعلوماتية السعودي ما بين (2.42 إلى 2.95)، وهي متوسطات تقع في الفئة الثالثة من فئات المقياس الثلاثي والتي تشير إلى "مدرك" في أداة الدراسة؛ مما يوضح التجانس في موافقة أفراد عينة الدراسة على مدى الوعي بالجرائم المعلوماتية المذكورة بنظام مكافحة الجرائم المعلوماتية السعودي.

وبناءً على ذلك تستنتج بأن أفراد عينة الدراسة مدركون للجرائم المعلوماتية المذكورة بنظام مكافحة الجرائم المعلوماتية السعودي بدرجة مرتفعة، حيث قد بلغ المتوسط الحسابي العام (2.79 من 3.00)، وهو متوسط يقع في الفئة الثالثة من فئات المقياس الثلاثي (من 2.34 إلى 3.00)، وهي الفئة التي تشير إلى خيار "مدرك" في أداة الدراسة.

وهذا مؤشر إيجابي مما يدل على أن أفراد عينة الدراسة لديهم ثقافة معلوماتية وقانونية فيما يتعلق بنظام مكافحة الجرائم المعلوماتية، ولكن من الضرورة الاستمرار برفع التوعية والتثقيف بشكل دوري لكافة أفراد عينة الدراسة؛ حيث كلما تطورت وتنوعت الجرائم المعلوماتية كلما أدى ذلك إلى تحديث بالنظام بشكل مستمر ليواكب كافة أنواع الجرائم المعلوماتية وأنماطها الناشئة والمستحدثة.

وفيما يلي ترتيباً تنازلياً لعبارات المحور حسب إدراك أفراد عينة الدراسة لها كالآتي:

1) جاءت العبارة رقم (6)، وهي " لا يحق لي الدخول الغير مشروع إلى موقع الكتروني أو نظام معلوماتي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني " بالمرتبة الأولى من حيث موافقة أفراد عينة الدراسة عليها بمتوسط (2.95 من 3).

2) جاءت العبارة رقم (3)، وهي " لا يحق لي الدخول الغير المشروع إلى الشبكة الالكترونية بهدف تهديد شخص أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه " بالمرتبة الثانية من حيث موافقة أفراد عينة الدراسة عليها بمتوسط (2.91 من 3).

3) جاءت العبارة رقم (7)، وهي "أدرك أن المساس بالحياة الخاصة من خلال إساءة استخدام الهواتف المحمولة يعرضني للمسؤولية" بالمرتبة الثالثة من حيث موافقة أفراد عينة الدراسة عليها بمتوسط (2.91 من 3).

4) جاءت العبارة رقم (14)، وهي " إنشاء أو نشر مواقع لمنظمات إرهابية على الشبكة المعلوماتية أو ترويج أفكارها وتمويلها يعاقب عليه نظام مكافحة جرائم المعلوماتية " بالمرتبة الرابعة من حيث موافقة أفراد عينة الدراسة عليها بمتوسط (2.91 من 3).

5) جاءت العبارة رقم (8)، وهي " أكون تحت طائلة المسؤولية إذا قمت بالتشهير بالآخرين وإلحاق الضرر بهم عبر وسائل تقنيات المعلومات " بالمرتبة الخامسة من حيث موافقة أفراد عينة الدراسة عليها بمتوسط (2.91 من 3).

6) جاءت العبارة رقم (11)، وهي "أكون تحت طائلة المسؤولية عند إنتاج محتوى ماس بالنظام العام، أو القيم الدينية ،أو الآداب العامة، وتخزينه على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي " بالمرتبة السادسة من حيث موافقة أفراد عينة الدراسة عليها بمتوسط (2.86 من 3).

7) جاءت العبارة رقم (13)، وهي " ينص النظام على منع نشر المواقع ذات الصلة بالمخدرات وترويجها والتسويق لها" بالمرتبة السابعة من حيث موافقة أفراد عينة الدراسة عليها بمتوسط (2.86 من 3).

8) جاءت العبارة رقم (5)، وهي " لا يحق لي الدخول الغير المشروع لإلغاء بيانات خاصة أو التلاعب بها أو إعادة نشرها " بالمرتبة الثامنة من حيث موافقة أفراد عينة الدراسة عليها بمتوسط (2.84 من 3).

9) جاءت العبارة رقم (12)، وهي "إنشاء وتداول البيانات المتعلقة بالشبكات الإباحية أو أنشطة الميسر المخلة بالآداب العامة يعاقب عليه نظام مكافحة جرائم المعلوماتية" بالمرتبة التاسعة من حيث موافقة أفراد عينة الدراسة عليها بمتوسط (2.84 من 3).

10) جاءت العبارة رقم (9)، وهي "الوصول غير المشروع إلى البيانات البنكية والخدمات البنكية المختلفة يعاقب عليه نظام مكافحة جرائم المعلوماتية" بالمرتبة العاشرة من حيث موافقة أفراد عينة الدراسة عليها بمتوسط (2.81 من 3).

11) جاءت العبارة رقم (10)، وهي " أدرك أن إعاقة الوصول إلى الخدمات عبر الشبكة المعلوماتية أو تعطيلها يعرضني للمسؤولية " بالمرتبة الحادية عشر من حيث موافقة أفراد عينة الدراسة عليها بمتوسط (2.70 من 3).

12) جاءت العبارة رقم (4)، وهي: " لا يحق لي الدخول الغير المشروع إلى أي موقع الكتروني دون إذن أو اختراقه " بالمرتبة الثانية عشر من حيث موافقة أفراد عينة الدراسة عليها بمتوسط (2.65 من 3).

13) جاءت العبارة رقم (1)، وهي: " أدرك أن نظام مكافحة جرائم المعلوماتية يعاقب على التنصت على المواد المرسلة عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي " بالمرتبة الثالثة عشر من حيث موافقة أفراد عينة الدراسة عليها بمتوسط (2.53 من 3).

14) جاءت العبارة رقم (2)، وهي: " يعاقب نظام مكافحة جرائم المعلوماتية من تسبب في إيقاف الشبكة المعلوماتية أو تعطيلها، أو مسح البرامج والبيانات المستخدمة فيها والتلاعب بها " بالمرتبة الرابعة عشر من حيث موافقة أفراد عينة الدراسة عليها بمتوسط (2.42 من 3)

❖ **التساؤل الثاني: ما أسباب ضعف الوعي بنظام مكافحة جرائم المعلوماتية السعودي من وجهة نظر طلاب وطالبات الدراسات العليا بكلية الآداب والعلوم الإنسانية في جامعة الملك عبدالعزيز؟**

للتعرف على أسباب ضعف الوعي بنظام مكافحة جرائم المعلوماتية السعودي تم حساب المتوسطات الحسابية، والانحرافات المعيارية، والترتيب لإجابات أفراد عينة الدراسة على المحور الثاني: من وجهة نظرك ماهي أسباب ضعف الوعي بنظام مكافحة جرائم المعلوماتية السعودي؟، وجاءت النتائج كما يوضحها الجدول الآتي:

العدد أربعون
تاريخ الإصدار: 2 – شباط – 2022 م
www.ajsp.net
ISSN: 2663-5798

جدول رقم (12)إجابات أفراد عينة الدراسة على المحور الثاني: من وجهة نظرك ماهي أسباب ضعف الوعي بنظام مكافحة جرائم المعلوماتية السعودي؟

رقم العبارة	العبارة	التكرار	درجة الاستجابة					المتوسط الحسابي	الانحراف المعياري	الترتيب
		النسبة	أثر ضعيف جداً	أثر ضعيف	أثر متوسط	مؤثر	مؤثر جداً			
1	قلة اهتمام أفراد المجتمع بنظام مكافحة جرائم المعلوماتية من خلال الاطلاع عليه ومعرفة مدى أهميته.	ك	5	16	67	74	155	1.87	1.015	1
		٪	1.6	5	21.1	23.3	48.9			
2	عدم وضوح صياغة الألفاظ والعبارات للنظام بشكل مناسب لكافة فئات المجتمع.	ك	19	52	67	110	69	2.50	1.174	4
		٪	6	16.4	21.1	34.7	21.8			
3	صعوبة فهم المواد المنصوصة بنظام مكافحة جرائم المعلوماتية وكيفية الأخذ بها.	ك	14	47	108	81	67	2.56	1.111	5
		٪	4.4	14.8	34.1	25.6	21.1			
4	عدم تثقيف أفراد المجتمع بنظام مكافحة جرائم المعلوماتية من قبل الجهات الأمنية المختصة.	ك	29	44	51	99	94	2.42	1.291	3
		٪	9.1	13.9	16.1	31.2	29.7			
5	قلة برامج التوعية والإثراء بالجرائم المعلوماتية وكيفية التعامل معها وفق التشريعات المحلية.	ك	25	36	54	86	116	2.27	1.278	2
		٪	7.9	11.4	17	27.1	36.6			
المتوسط الحسابي العام – الانحراف المعياري العام								2.32	0,815	

يتضح من الجدول رقم (12) ما يأتي:

من خلال النتائج الموضحة أعلاه يتضح أن هناك تجانس في موافقة أفراد عينة الدراسة على أسباب ضعف الوعي بنظام مكافحة جرائم المعلوماتية السعودي، حيث تراوحت متوسطات موافقتهم على أسباب ضعف الوعي بنظام مكافحة جرائم المعلوماتية السعودي ما بين (1.87 إلى 2.56)، وهي متوسطات تقع في الفئة الثانية من فئات المقياس الخماسي والتي تشير إلى "مؤثر " في أداة الدراسة؛ مما يوضح التجانس في موافقة أفراد عينة الدراسة على أسباب ضعف الوعي بنظام مكافحة جرائم المعلوماتية السعودي.

وبالنظر إلى متوسطات استجابات أفراد العينة لعبارات المحور، نجد أن العبارة رقم (1) التي تنص على (قلة اهتمام أفراد المجتمع بنظام مكافحة جرائم المعلوماتية من خلال الاطلاع عليه ومعرفة مدى أهميته) قد احتلت المرتبة الأولى من حيث موافقة أفراد عينة الدراسة عليها بمتوسط (1.87 من 5). حيث تعتبر أنها من الأسباب الأكثر أثراً من بين التي تم ذكرها بالمحور، وتشير هذه النتيجة إلى ضرورة ارشاد الأفراد بالاطلاع على نظام مكافحة جرائم المعلوماتية وبيان أهمية النظام؛ حيث يساهم النظام إلى تقليص حجم الجرائم المعلوماتية، وذلك بفرض العقوبات للحد منها، إذ يسعى للوصول إلى الأمن المعلوماتي وتحقيقه والحفاظ على الحقوق الناتجة عن الاستخدام القانوني لتقنية المعلومات.

وفي ضوء ذلك نستنتج أن أفراد عينة الدراسة موافقون بدرجة مرتفعة على أن هناك أسباب لها أثر على ضعف الوعي بنظام مكافحة جرائم المعلوماتية السعودي بمتوسط (2.32 من 5.00)، وهو متوسط يقع في الفئة الثانية من فئات المقياس الخماسي (من 1.81 إلى 2.60)، وهي الفئة التي تشير إلى خيار "مؤثر" في أداة الدراسة.

وفي ذات السياق نرى أن أغلب هذه الأسباب يمكن حلها عن طريق زيادة برامج التوعية والإثراء بالجرائم المعلوماتية وكيفية التعامل معها وفق التشريعات المحلية؛ يجب على الجهات الأمنية المختصة القيام بإرشاد وتوعية كافة أفراد المجتمع بالنظام بشكل دوري ومستمر؛ القيام بمبادرات توعوية لإيضاح المواد المنصوصة بنظام مكافحة الجرائم المعلوماتية وكيفية الأخذ بها بشكل سلس ومناسب لكافة فئات المجتمع.

وفيما يلي ترتيباً تنازلياً لعبارات المحور حسب السبب الأكثر أثراً كالآتي:

1. جاءت العبارة رقم (1)، وهي" قلة اهتمام أفراد المجتمع بنظام مكافحة جرائم المعلوماتية من خلال الاطلاع عليه ومعرفة مدى أهميته" بالمرتبة الأولى من حيث موافقة أفراد عينة الدراسة عليها أنها مؤثرة بمتوسط (1.87 من5).
2. جاءت العبارة رقم (5)، وهي " قلة برامج التوعية والإثراء بالجرائم المعلوماتية وكيفية التعامل معها وفق التشريعات المحلية " بالمرتبة الثانية من حيث موافقة أفراد عينة الدراسة عليها أنها مؤثرة بمتوسط (2.27 من 5).
3. جاءت العبارة رقم (4)، وهي " عدم تثقيف أفراد المجتمع بنظام مكافحة جرائم المعلوماتية من قبل الجهات الأمنية المختصة " بالمرتبة الثالثة من حيث موافقة أفراد عينة الدراسة عليها أنها مؤثرة بمتوسط (2.42 من 5).
4. جاءت العبارة رقم (2)، وهي " عدم وضوح صياغة الألفاظ والعبارات للنظام بشكل مناسب لكافة فئات المجتمع " بالمرتبة الرابعة من حيث موافقة أفراد عينة الدراسة أنها مؤثرة بمتوسط (2.50 من 5).
5. جاءت العبارة رقم (3)، وهي " صعوبة فهم المواد المنصوصة بنظام مكافحة جرائم المعلوماتية وكيفية الأخذ بها " بالمرتبة الخامسة من حيث موافقة أفراد عينة الدراسة أنها مؤثرة بمتوسط (2.56 من 5).

وقد أشار البعض من أفراد العينة بنسبة (4.8%) أن هناك أسباب أخرى لضعف الوعي بنظام مكافحة جرائم المعلوماتية السعودي حسب وجهة نظرهم والتي تتمثل في الآتي: جهل بعض أفراد المجتمع بأن الفضاء المعلوماتي لديه قوانين وتشريعات محلية؛ عدم حل

العدد أربعون
تاريخ الإصدار: 2 – شباط – 2022 م
www.ajsp.net
ISSN: 2663-5798

المشكلة الأساسية التي أدت إلى ارتكاب الجريمة المعلوماتية. حيث نرى أنها أسباب مؤثرة، كما أن جميع هذه الأسباب قد يكون حلها الأساسي هو القيام بمبادرات توعوية لنظام مكافحة الجرائم المعلوماتية السعودي لرفع مستوى الوعي بها.

❖ **التساؤل الثالث: ما هي أبرز الطرق للمكافحة والوقاية من الجرائم المعلوماتية في ظل التحول الرقمي تماشياً مع رؤية 2030 من وجهة نظر طلاب وطالبات الدراسات العليا بكلية الآداب والعلوم الإنسانية في جامعة الملك عبدالعزيز ؟**

للتعرف على أبرز الطرق للمكافحة والوقاية من الجرائم المعلوماتية في ظل التحول الرقمي تماشياً مع رؤية 2030 تم حساب المتوسطات الحسابية، والانحرافات المعيارية، والترتيب لإجابات أفراد عينة الدراسة على المحور الثالث: من وجهة نظرك ماهي أبرز الطرق للمكافحة والوقاية من الجرائم المعلوماتية في ظل التحول الرقمي تماشياً مع رؤية 2030؟، وجاءت النتائج كما يوضحها الجدول الآتي:

جدول رقم (13) إجابات أفراد عينة الدراسة على المحور الثالث: من وجهة نظرك ماهي أبرز الطرق للمكافحة والوقاية من الجرائم المعلوماتية في ظل التحول الرقمي تماشياً مع رؤية 2030؟

رقم العبارة	العبارة	التكرار	درجة الاستجابة			المتوسط الحسابي	الانحراف المعياري	الترتيب
		النسبة	موافق	محايد	غير موافق			
1	تفعيل تقنية التوقيع الالكتروني وتطبيقها في كافة الخدمات الحكومية وغيرها، لرفع مستوى الموثوقية ومنع إساءة الاستخدام والاحتيال في التعاملات الالكترونية	ك	232	77	8	2.71	0.509	9
		٪	73.2	24.3	2.5			
2	تطوير برمجيات آمنة ونظم تشغيل قوية التي تحد من الاختراقات الإلكترونية	ك	303	13	1	2.95	0.227	1
		٪	95.6	4.1	0.3			
3	تشجيع الهيئات على استخدام التشفير الوطني للبيانات للمساهمة في حماية البيانات والأنظمة والشبكات الوطنية	ك	278	34	5	2.86	0.389	7
		٪	87.7	10.7	1.6			
4	مواكبة التطورات المرتبطة بالجريمة المعلوماتية والحرص على تطوير وسائل مكافحتها	ك	295	22	0	2.93	0.255	2
		٪	93.1	6.9	0			

العدد أربعون
تاريخ الإصدار: 2 – شباط – 2022 م
www.ajsp.net
ISSN: 2663-5798

رقم العبارة	العبارة	التكرار	درجة الاستجابة			المتوسط الحسابي	الانحراف المعياري	الترتيب
		النسبة	موافق	محايد	غير موافق			
5	تثقيف أفراد المجتمع بضرورة إبلاغ الجهات الأمنية المختصة في حال التعرض لجريمة معلوماتية	ك	296	18	3	2.92	0.299	5
		٪	93.4	5.7	0.9			
6	القيام بمبادرات تقدم دورات تدريبية وورش تعليمية لمكافحة الجرائم المعلوماتية مجاناً لكافة شرائح المجتمع	ك	273	39	5	2.85	0.403	8
		٪	86.1	12.3	1.6			
7	تثقيف أفراد المجتمع بالأساليب الصحيحة والآمنة عند استخدام الشبكة الإلكترونية	ك	293	23	1	2.92	0.281	4
		٪	92.4	7.3	0.3			
8	تأسيس وحدة أمنية خاصة لمكافحة الجرائم المعلوماتية والحد منها	ك	291	25	1	2.91	0.291	6
		٪	91.8	7.9	0.3			
9	زيادة برامج التوعية والإثراء بالجرائم المعلوماتية وكيفية التعامل معها وفق التشريعات المحلية	ك	296	20	1	2.93	0.267	3
		٪	93.4	6.3	0.3			
المتوسط الحسابي العام – الانحراف المعياري العام						**2.89**	**0.208**	

يتضح من الجدول رقم (13) ما يأتي:

أن هناك تجانس في موافقة أفراد عينة الدراسة على أبرز الطرق للمكافحة والوقاية من الجرائم المعلوماتية في ظل التحول الرقمي تماشياً مع رؤية 2030، حيث تراوحت متوسطات موافقتهن على أبرز الطرق للمكافحة والوقاية من الجرائم المعلوماتية في ظل التحول الرقمي تماشياً مع رؤية 2030 ما بين (2.71 إلى 2.34)، وهي متوسطات تقع في الفئة الثالثة من فئات المقياس الثلاثي والتي تشير إلى "موافق" في أداة الدراسة؛ مما يوضح التجانس في موافقة أفراد عينة الدراسة على أبرز الطرق للمكافحة والوقاية من الجرائم المعلوماتية في ظل التحول الرقمي تماشياً مع رؤية 2030.

وبالنظر إلى متوسطات استجابات أفراد العينة لعبارات المحور، نجد أن العبارة رقم (2) التي تنص على (تطوير برمجيات آمنة ونظم تشغيل قوية التي تحد من الاختراقات الإلكترونية) قد احتلت المرتبة الأولى من حيث درجة موافقة أفراد عينة الدراسة عليها، وهذا يدل إلى حاجة أفراد العينة إلى برمجيات ونظم تشغيل قوية وآمنة لأجهزتهم مما يؤدي ذلك إلى تقليل الاختراقات الالكترونية. كما نجد عبارة رقم (1) التي تنص على (تفعيل تقنية التوقيع الالكتروني وتطبيقها في كافة الخدمات الحكومية وغيرها، لرفع مستوى الموثوقية ومنع إساءة الاستخدام والاحتيال في التعاملات الالكترونية) قد احتلت المرتبة الأخيرة من حيث درجة موافقة أفراد عينة الدراسة عليها، وقد يعود سبب هذه النتيجة إلى أن البعض ليس لديهم معرفة سابقة في استخدام تقنية التوقيع الالكتروني خوفاً من احتمالية الإساءة في استخدامها أو ارتفاع تكلفتها.

وبناء على ذلك نستنتج أن أفراد عينة الدراسة موافقون بدرجة مرتفعة على أبرز الطرق للمكافحة والوقاية من الجرائم المعلوماتية في ظل التحول الرقمي تماشياً مع رؤية 2030بمتوسط (2.89 من 3.00)، وهو متوسط يقع في الفئة الثالثة من فئات المقياس الثلاثي (من 2.34 إلى 3.00)، وهي الفئة التي تشير إلى خيار "موافق" في أداة الدراسة. وهذا مؤشر إيجابي حيث نأمل من الجهات المختصة الأخذ بهذه الطرق ومراعاتها لمكافحة الجرائم المعلوماتية والوقاية منها.

وفيما يلي ترتيباً تنازلياً لعبارات المحور حسب موافقة أفراد عينة الدراسة عليها كالآتي:

1) جاءت العبارة رقم (2)، وهي: " تطوير برمجيات آمنة ونظم تشغيل قوية التي تحد من الاختراقات الإلكترونية" بالمرتبة الأولى من حيث موافقة أفراد عينة الدراسة عليها بمتوسط (2.95 من 3).
2) جاءت العبارة رقم (4)، وهي: " مواكبة التطورات المرتبطة بالجريمة المعلوماتية والحرص على تطوير وسائل مكافحتها " بالمرتبة الثانية من حيث موافقة أفراد عينة الدراسة عليها بمتوسط (2.93 من 3).
3) جاءت العبارة رقم (9)، وهي: " زيادة برامج التوعية والإثراء بالجرائم المعلوماتية وكيفية التعامل معها وفق التشريعات المحلية " بالمرتبة الثالثة من حيث موافقة أفراد عينة الدراسة عليها بمتوسط (2.93 من 3).
4) جاءت العبارة رقم (7)، وهي: " تثقيف أفراد المجتمع بالأساليب الصحيحة والآمنة عند استخدام الشبكة الإلكترونية " بالمرتبة الرابعة من حيث موافقة أفراد عينة الدراسة عليها بمتوسط (2.92 من 3).
5) جاءت العبارة رقم (5)، وهي: " تثقيف أفراد المجتمع بضرورة إبلاغ الجهات الأمنية المختصة في حال التعرض لجريمة معلوماتية " بالمرتبة الخامسة من حيث موافقة أفراد عينة الدراسة عليها بمتوسط (2.92 من 3).
6) جاءت العبارة رقم (8)، وهي: " تأسيس وحدة أمنية خاصة لمكافحة الجرائم المعلوماتية والحد منها " بالمرتبة السادسة من حيث موافقة أفراد عينة الدراسة عليها بمتوسط (2.91 من 3).
7) جاءت العبارة رقم (3)، وهي: " تشجيع الهيئات على استخدام التشفير الوطني للبيانات للمساهمة في حماية البيانات والأنظمة والشبكات الوطنية " بالمرتبة السابعة من حيث موافقة أفراد عينة الدراسة عليها بمتوسط (2.86 من 3).
8) جاءت العبارة رقم (6)، وهي: " القيام بمبادرات تقدم دورات تدريبية وورش تعليمية لمكافحة الجرائم المعلوماتية مجاناً لكافة شرائح المجتمع " بالمرتبة الثامنة من حيث موافقة أفراد عينة الدراسة عليها بمتوسط (2.85 من 3).

9) جاءت العبارة رقم (1)، وهي: " تفعيل تقنية التوقيع الالكتروني وتطبيقها في كافة الخدمات الحكومية وغيرها، لرفع مستوى الموثوقية ومنع إساءة الاستخدام والاحتيال في التعاملات الالكترونية " بالمرتبة التاسعة من حيث موافقة أفراد عينة الدراسة عليها بمتوسط (2.71 من 3).

وقد أشار البعض من أفراد العينة بنسبة (3%) أن هناك طرق أخرى للمكافحة والوقاية من الجرائم المعلوماتية في ظل التحول الرقمي تماشياً مع رؤية 2030 حسب وجهة نظرهم والتي تتمثل في استخدام تقنية Blockchain للحد من التلاعب بالهوية؛ توعية أفراد المجتمع بالجرائم المعلوماتية وأنظمة مكافحتها عن طريق برامج الراديو، وتطبيقات التواصل الاجتماعي؛ تأسيس منصة خاصة بالجرائم المعلوماتية يتم من خلالها رفع العقوبات التي أخذت صفة قطعية ونشرها؛ التشهير بالمجرم المعلوماتي؛ إدراج اللوائح والقوانين في حساب المواطن عبر بوابة ابشر وأخذ تعهد بعد كل ستة أشهر ليضل المواطن على وعي مستمر. إذ تعتبر طرق صحيحة وجيدة حيث نأمل من الجهات المختصة الأخذ بها ومراعاتها لمكافحة الجرائم المعلوماتية والوقاية منها.

❖ **التساؤل الرابع: ما مدى الوعي بأدوات الإبلاغ عن الجرائم المعلوماتية في المملكة العربية السعودية لدى طلاب وطالبات الدراسات العليا بكلية الآداب والعلوم الإنسانية في جامعة الملك عبدالعزيز ؟**

للتعرف على مدى الوعي بأدوات الإبلاغ عن الجرائم المعلوماتية في المملكة العربية السعودية تم حساب المتوسطات الحسابية، والانحرافات المعيارية، والترتيب لإجابات أفراد عينة الدراسة على المحور الرابع: هل لديك معرفة بأنه يمكنك الإبلاغ عن الجرائم المعلوماتية من خلال أحد الأدوات التالية؟، وجاءت النتائج كما يوضحها الجدول الآتي:

جدول رقم (14) إجابات أفراد عينة الدراسة على المحور الرابع: هل لديك معرفة بأنه يمكنك الإبلاغ عن الجرائم المعلوماتية من خلال أحد الأدوات التالية؟

رقم العبارة	العبارة	التكرار	درجة الاستجابة			المتوسط الحسابي	الانحراف المعياري	الترتيب
		النسبة	مدرك	مدرك إلى حد ما	غير مدرك			
1	إرسال البلاغ عبر تطبيق كلنا أمن على الأجهزة الذكية التابع للأمن العام.	ك	232	46	39	2.61	0.697	2
		٪	73.2	14.5	12.3			
2	البلاغ من خلال أقرب مركز الشرطة.	ك	229	54	34	2.62	0.673	1
		٪	72.2	17.0	10.7			

العدد أربعون
تاريخ الإصدار: 2 – شباط – 2022 م
www.ajsp.net
ISSN: 2663-5798

رقم العبارة	العبارة	التكرار	درجة الاستجابة			المتوسط الحسابي	الانحراف المعياري	الترتيب
		النسبة	مدرك	مدرك إلى حد ما	غير مدرك			
3	الاتصال على الرقم 989.	ك	104	74	139	1.89	0.870	4
		٪	32.8	23.3	43.8			
4	البريد الإلكتروني: info.cybercrime@moisp.gov.sa	ك	65	69	183	1.63	0.804	5
		٪	20.5	21.8	57.7			
5	رفع البلاغ عبر البوابة الإلكترونية لوزارة الداخلية(أبشر).	ك	117	73	127	1.97	0.878	3
		٪	36.9	23.0	40.1			
المتوسط الحسابي العام – الانحراف المعياري العام						2.14	0.565	

يتضح من الجدول رقم (14) ما يأتي:

أن هناك تفاوت في موافقة أفراد عينة الدراسة على مدى الوعي بأدوات الإبلاغ عن الجرائم المعلوماتية في المملكة العربية السعودية، حيث تراوحت متوسطات موافقتهن على مدى الوعي بأدوات الإبلاغ عن الجرائم المعلوماتية في المملكة العربية السعودية ما بين (1.63 إلى 2.62)، وهي متوسطات تقع في الفئتين الأولى والثالثة من فئات المقياس الثلاثي واللتان تشيران إلى "غير مدرك – مدرك" في أداة الدراسة؛ مما يوضح التفاوت في موافقة أفراد عينة الدراسة على مدى الوعي بأدوات الإبلاغ عن الجرائم المعلوماتية في المملكة العربية السعودية، وهذا قد يعود إلى ثقافة الطلبة واطلاعهم على ما ينشر حول كيفية التعامل مع الجرائم المعلوماتية وفق التشريعات المحلية؛ تحديداً في معرفة الطرق الحديثة للإبلاغ عن الجرائم المعلوماتية في السعودية.

في حين يتضح من النتائج أن أفراد عينة الدراسة مدركون لإثنين من أدوات الإبلاغ عن الجرائم المعلوماتية في المملكة العربية تتمثلان في العبارتين رقم (2 ، 1)، واللتين تم ترتيبهما تنازلياً حسب إدراك أفراد عينة الدراسة لهما كالآتي:

1) جاءت العبارة رقم (2)، وهي " البلاغ من خلال أقرب مركز الشرطة " بالمرتبة الأولى من حيث إدراك أفراد عينة الدراسة لها بمتوسط (2.62 من 3).

2) جاءت العبارة رقم (1)، وهي " إرسال البلاغ عبر تطبيق كلنا أمن على الأجهزة الذكية التابع للأمن العام " بالمرتبة الثانية من حيث إدراك أفراد عينة الدراسة لها بمتوسط (2.61 من 3).

بينما يتضح من النتائج أن أفراد عينة الدراسة مدركون إلى حد ما لأثنين من أدوات الإبلاغ عن الجرائم المعلوماتية في المملكة العربية تتمثلان في العبارتين رقم (5 ، 3)، واللتين تم ترتيبهما تنازلياً حسب إدراك أفراد عينة الدراسة لهما إلى حدما كالآتي:

3) جاءت العبارة رقم (5)، وهي " رفع البلاغ عبر البوابة الإلكترونية لوزارة الداخلية(أبشر)." بالمرتبة الأولى من حيث إدراك أفراد عينة الدراسة لها إلى حدما بمتوسط (1.97 من 3).

4) جاءت العبارة رقم (3)، وهي" الاتصال على الرقم 989." بالمرتبة الثانية من حيث إدراك أفراد عينة الدراسة لها إلى حدما بمتوسط (1.89 من 3).

ويتضح من النتائج أن أفراد عينة الدراسة غير مدركون لواحدة من أدوات الإبلاغ عن الجرائم المعلوماتية في المملكة العربية تتمثل في العبارة رقم (4)، وهي " البريد الإلكتروني: info.cybercrime@moisp.gov.sa ." بمتوسط (1.63 من 3). ولعل عدم إدراك أفراد عينة الدراسة بها قد يعود إلى قلة الاقبال في الإبلاغ عن طريق البريد الالكتروني مما أدى إلى عدم انتشارها.

وبناءً على ذلك نستنتج أن أفراد عينة الدراسة مدركون إلى حد ما لأدوات الإبلاغ عن الجرائم المعلوماتية في المملكة العربية بمتوسط (2.14 من 3.00)، وهو متوسط يقع في الفئة الثانية من فئات المقياس الثلاثي (من 1.67 إلى 2.33)، وهي الفئة التي تشير إلى خيار "مدرك إلى حد ما" في أداة الدراسة. وتعتبر نتيجة متوسطة لذلك يجب على الجهات المختصة القيام بزيادة برامج التثقيف والتوعية بأدوات الابلاغ عن الجرائم المعلوماتية المملكة العربية السعودية.

3. النتائج والتوصيات

أولاً: النتائج:

أسفرت الدراسة إلى مجموعة من النتائج، يمكن إجمالها فيما يلي:

1. توصلت الدراسة إلى أن مستوى الوعي بالجرائم المعلوماتية المذكورة بنظام مكافحة الجرائم المعلوماتية السعودي قد بلغ درجة مرتفعة لدى أفراد عينة الدراسة، بمتوسط حسابي قدره (2.79).
2. بينت احصائيات الدراسة أن أفراد عينة الدراسة لديهم معرفة وثقافة قانونية عالية فيما يتعلق بنظام مكافحة جرائم المعلوماتية السعودي.
3. كشفت الدراسة أسباب ضعف الوعي بنظام مكافحة جرائم المعلوماتية السعودي حسب وجهة نظر أفراد عينة الدراسة، وتتمثل على النحو الآتي:

- قلة اهتمام أفراد المجتمع بنظام مكافحة جرائم المعلوماتية من خلال الاطلاع عليه ومعرفة مدى أهميته.
- قلة برامج التوعية والإثراء بالجرائم المعلوماتية وكيفية التعامل معها وفق التشريعات المحلية.
- عدم وضوح صياغة الألفاظ والعبارات للنظام بشكل مناسب لكافة فئات المجتمع.
- عدم تثقيف أفراد المجتمع بنظام مكافحة جرائم المعلوماتية من قبل الجهات الأمنية المختصة.
- صعوبة فهم المواد المنصوصة بنظام مكافحة جرائم المعلوماتية وكيفية الأخذ بها.
- جهل بعض أفراد المجتمع بأن الفضاء المعلوماتي لديه قوانين وتشريعات محلية.
- عدم حل المشكلة الأساسية التي أدت إلى ارتكاب الجريمة المعلوماتية.

4. تبين من الدراسة أن من أسباب ضعف الوعي بنظام مكافحة جرائم المعلوماتية السعودي الأكثر أثراً حسب وجهة نظر أفراد العينة هو قلة اهتمام أفراد المجتمع بنظام مكافحة جرائم المعلوماتية من خلال الاطلاع عليه ومعرفة مدى أهميته.
5. كشفت الدراسة عن أبرز طرق المكافحة والوقاية من الجرائم المعلوماتية في ظل التحول الرقمي تماشياً مع رؤية 2030 حسب وجهة نظر أفراد عينة الدراسة، وتتمثل على النحو الآتي:

- تطوير برمجيات آمنة ونظم تشغيل قوية التي تحد من الاختراقات الإلكترونية.
- مواكبة التطورات المرتبطة بالجريمة المعلوماتية والحرص على تطوير وسائل مكافحتها.
- زيادة برامج التوعية والإثراء بالجرائم المعلوماتية وكيفية التعامل معها وفق التشريعات المحلية .
- تثقيف أفراد المجتمع بالأساليب الصحيحة والآمنة عند استخدام الشبكة الإلكترونية .
- تثقيف أفراد المجتمع بضرورة إبلاغ الجهات الأمنية المختصة في حال التعرض لجريمة معلوماتية.
- تأسيس وحدة أمنية خاصة لمكافحة الجرائم المعلوماتية والحد منها.
- تشجيع الهيئات على استخدام التشفير الوطني للبيانات للمساهمة في حماية البيانات والأنظمة والشبكات الوطنية.
- القيام بمبادرات تقدم دورات تدريبية وورش تعليمية لمكافحة الجرائم المعلوماتية مجاناً لكافة شرائح المجتمع.
- تفعيل تقنية التوقيع الالكتروني وتطبيقها في كافة الخدمات الحكومية وغيرها، لرفع مستوى الموثوقية ومنع إساءة الاستخدام والاحتيال في التعاملات الالكترونية.
- استخدام تقنية Blockchain للحد من التلاعب بالهوية.
- توعية أفراد المجتمع بالجرائم المعلوماتية وأنظمة مكافحتها عن طريق برامج الراديو، وتطبيقات التواصل الاجتماعي.
- تأسيس منصة خاصة بالجرائم المعلوماتية يتم من خلالها رفع العقوبات التي أخذت صفة قطعية ونشرها؛ والتشهير بالمجرم المعلوماتي.
- إدراج اللوائح والقوانين في حساب المواطن عبر بوابة ابشر وأخذ تعهد بعد كل ستة أشهر ليضل المواطن على وعي مستمر.

6. بينت احصائيات الدراسة أن تطوير برمجيات آمنة ونظم تشغيل قوية التي تحد من الاختراقات الإلكترونية تحتل المرتبة الأولى من طرق مكافحة الجرائم المعلوماتية حسب وجهة نظر أفراد العينة.
7. أظهرت الدراسة إلى أن مستوى المعرفة والوعي بأدوات الإبلاغ عن الجرائم المعلوماتية في المملكة العربية السعودية قد بلغ درجة متوسطة لدى أفراد عينة الدراسة، بمتوسط حسابي قدره (2.14).
8. كشفت الدراسة عدم معرفة أفراد عينة الدراسة لواحدة من أدوات الإبلاغ عن الجرائم المعلوماتية في المملكة العربية وهي (البريد الإلكتروني: info.cybercrime@moisp.gov.sa).

ثانياً: التوصيات:

في ضوء النتائج التي توصلت إليها الدراسة توصي بالآتي:

1- ضرورة تطوير وتحديث نظام مكافحة الجرائم المعلوماتية السعودي بشكل مستمر ليواكب كافة أنواع الجرائم المعلوماتية وأنماطها الناشئة والمستحدثة.

2- ينبغي على الجهات المختصة القيام بمبادرات توعوية تساهم في توعية أفراد المجتمع بما يتعلق بالجرائم المعلوماتية وأنظمة مكافحتها بشكل دوري ومستمر لرفع مستوى ثقافة المجتمع.

3- يجب على الجهات المختصة الأخذ بالاعتبار بأبرز طرق المكافحة والوقاية من الجرائم المعلوماتية في ظل التحول الرقمي تماشياً مع رؤية 2030 التي توصلت إليها الدراسة.

4- تثقيف وتوعية أفراد المجتمع بأدوات الإبلاغ عن الجرائم المعلوماتية في المملكة العربية السعودية باعتماد طرق وأساليب متنوعة كمقاطع الفيديو، والمطويات، والنشرات ...الخ.

5- ضرورة توحيد طرق مكافحة الجرائم المعلوماتية والوقاية منها؛ للحد من انتشار الجرائم المعلوماتية.

6- أهمية إدراج موضوع الجرائم المعلوماتية ضمن المقررات الدراسية التي لها علاقة بها؛ وذلك لإكساب الطلاب والطالبات مهارات الحماية من مخاطر الجرائم المعلوماتية وكيفية التعامل معها وفق التشريعات المحلية.

7- إجراء دراسات علمية لمعرفة مستوى وعي الطلبة بنظام مكافحة جرائم المعلوماتية ولإثراء الإنتاج الفكري العربي.

8- إجراء دراسات علمية متخصصة لمعرفة جهود المملكة العربية السعودية في مكافحة الجرائم المعلوماتية.

قائمة المراجع:

- **المراجع العربية:**

أصيل، غادة عبدالوهاب، وخضري، هيفاء طلعت. (2016). **مدى الوعي بالجرائم المعلوماتية بين مستخدمي مواقع التواصل الاجتماعي: دراسة مسحية على مدينة جدة**. 1- 45.

آل جار الله، عبدالعزيز بن غرم الله بن جار الله. (2017). **جرائم الإنترنت وعقوباتها وفق نظام مكافحة جرائم المعلوماتية السعودي (ويليه آثار العولمة على مستخدمي الإنترنت)**. الرياض: دار الكتاب الجامعي للنشر والتوزيع، ط 1، 483ص.

بن لعامر، وليد. (2021). **الجريمة المعلوماتية ضد الطفولة : جريمة تتحدى الواقع وتسابق التشريع**. المجلة الجزائرية للأمن والتنمية، مج 10، ع 3، 802 – 813. مسترجع من https://search.emarefa.net/detail/BIM-1246184

بنوان، هبة إبراهيم الشحات، المنوفي، محمد إبراهيم، والجندي، ياسر مصطفى. (2016). **الجامعة وتنمية وعي طلابها بالجرائم الإلكترونية في ضوء التطور التقني والمعلوماتي**. مجلة كلية التربية: جامعة كفر الشيخ – كلية التربية، مج16، ع3 ، 149 – 180. مسترجع من http://search.mandumah.com/Record/1002901

الخطيب، أحمد حسن عبد العليم حسن. (2019). **الجرائم المعلوماتية الواقعة عبر مواقع التواصل الاجتماعي قراءة في قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018 ونظام مكافحة جرائم المعلوماتية السعودي 1428 هـ**. المجلة القانونية: جامعة القاهرة – كلية الحقوق – فرع الخرطوم، مج6، ع1، 67 – 94. مسترجع من http://search.mandumah.com/Record/1032589

الخطيب، أحمد حسن عبد العليم حسن. (2019). **الجرائم المعلوماتية الواقعة عبر مواقع التواصل الاجتماعي قراءة في قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018 ونظام مكافحة جرائم المعلوماتية السعودي 1428 هـ**. المجلة

القانونية: جامعة القاهرة – كلية الحقوق – فرع الخرطوم، مج6، ع1، 67 – 94. مسترجع من http://search.mandumah.com/Record/1032589

الدوسري، محمد. (2021). **الجرائم المعلوماتية**. مدونة محمد الدوسري. مسترجع من https://cutt.us/9shsC

الربيعة، صالح بن علي بن عبد الرحمن. (د.ت). **الجريمة المعلوماتية مخاطرها وعقوباتها**. هيئة الاتصالات وتقنية المعلومات، 1-33. مسترجع من https://attachments-us1-cloud-deskpro-com.s3.amazonaws.com/files/7102/2639/2638967SMSMWTKMDCHGBHG0--.pdf

سعيد، أميمة دسوقي محمد. (2019). **الوعي المجتمعي بالجرائم المعلوماتية لدى الطالبة الجامعية: دراسة من منظور تنظيم المجتمع في الخدمة الاجتماعية**. مجلة الخدمة الاجتماعية: الجمعية المصرية للأخصائيين الاجتماعيين، ع61، ج3 ، 335 – 375.مسترجع من http://search.mandumah.com/Record/989071

عبدالرازق، رانا مصباح عبدالمحسن. (2021). **تأثير الذكاء الاصطناعي على الجريمة الإلكترونية**. المجلة العلمية لجامعة الملك فيصل – العلوم الإنسانية والإدارية: جامعة الملك فيصل، مج22, ع1 ، 430 – 437. مسترجع من http://search.mandumah.com/Record/1091336

عمارة، فتيحة (2019). **الجريمة المعلوماتية**. مجلة أبحاث قانونية: جامعة التحدي – كلية القانون، ع7، 77 – 98. مسترجع من http://search.mandumah.com/Record/1021457

غريب، ماجدة عزت، والأمير، حسن. (2017). **مدى الوعي لدى الفئة العمرية الشابة بنظام عقوبات الجرائم المعلوماتية السعودي**. المجلة العربية الدولية للمعلوماتية: اتحاد الجامعات العربية – جمعية كليات الحاسبات والمعلومات، مج5، ع9 ، 17 – 32. مسترجع من http://search.mandumah.com/Record/866016

متولي، أحمد حسني صالح. (2015). **الجرائم المعلوماتية (2.0): رؤية مقترحة من منظور تربوي لدور أعضاء هيئة التدريس بكليات التربية لزيادة الوعي بمكافحة الجرائم المعلوماتية. المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية– ICACC: جامعة الإمام محمد بن سعود الإسلامية – كلية علوم الحاسب والمعلومات، المملكة العربية السعودية**. الرياض: جامعة الإمام محمد بن سعود الإسلامية. كلية علوم الحاسب والمعلومات، 184 – 194. مسترجع من http://search.mandumah.com/Record/690639

المطوع، عبد الله بن سعود بن سليمان. (2021). **مستوى الوعي لدى طلبة كلية التربية بشقراء بجامعة شقراء بنظام مكافحة جرائم المعلوماتية والتدابير التربوية لزيادته**. مجلة العلوم التربوية: جامعة الامام محمد بن سعود الإسلامية، مج1، ع24، 293 – 369. مسترجع من http://212.138.118.109/index.php/joes/article/view/1329

المقصودي، محمد بن أحمد بن علي. (2017). **الجرائم المعلوماتية: خصائصها وكيفية مواجهتها قانونياً**. المجلة العربية للدراسات الأمنية: جامعة نايف العربية للعلوم الأمنية، مج33، ع70، 101 – 131. مسترجع من http://search.mandumah.com/Record/865436

المنصة الوطنية الموحدة GOV.SA. (2021). **بلاغ عن الجرائم الإلكترونية**. مسترجع من https://www.my.gov.sa/wps/portal/snp/servicesDirectory/servicedetails/6166

المنصة الوطنية الموحدة GOV.SA. (د.ت). **البلاغات الأمنية (تطبيق كلنا أمن)**. مسترجع من https://www.my.gov.sa/wps/portal/snp/servicesDirectory/servicedetails/10262

نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية، مرسوم ملكي رقم: م/ 17 بتاريخ 8 / 3 / 1428هـ، ساري. مسترجع من https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/25df73d6-0f49-4dc5-b010-a9a700f2ec1d/1

الهيف، عالية بنت مذكر، والعنزي، دلال. (2018). **الجرائم المعلوماتية أنواعها وخطورتها: دراسة لقياس مستوى وعي طلبات قسم المكتبات والمعلومات في جامعة الأميرة نورة بنت عبدالرحمن 1438 هـ - 1439 / 2017 – 2018**. المجلة الأردنية للمكتبات والمعلومات: جمعية المكتبات والمعلومات الأردنية، مج53، ع3، 45 – 91. مسترجع من http://search.mandumah.com/Record/922801

هيئة الاتصالات وتقنية المعلومات (2017). **التقرير السنوي 1438-1439**، 116-122. مسترجع من https://www.citc.gov.sa/ar/mediacenter/annualreport/Documents/PR_REP_013A.pdf

وحدة التحول الرقمي. (2021). **التحول الرقمي**. مسترجع من https://ndu.gov.sa/about.php

اليحيى، تركي بن محمد بن عبدالرحمن. (2013). **مكافحة جرائم المعلوماتية في المملكة العربية السعودية**. مجلة البحوث والدراسات الشرعية: عبد الفتاح محمود ادريس، مج 2، ع 7، 253 – 288. مسترجع من http://search.mandumah.com/Record/338233

المراجع الأجنبية:

Alabdulatif, A. (2018). **Cybercrime and Analysis of Laws in Kingdom of Saudi Arabia.** Unpublished Ph.D. Texas: University of Houston,1 – 71. Available At: https://uh-ir.tdl.org/handle/10657/3107

Alghamdi, M. I. (2020). **A Strategic Vision to Reduce Cybercrime to Enhance Cyber Security**. Webology, 17(2), 289 - 295. Available At: https://webology.org/data-cms/articles/20201217052841pmWEB17031.pdf

Almrezeq, N., Alserhani, F. and Humayun, M. (2021). **Exploratory Study to Measure Awareness of Cybercrime in Saudi Arabia**. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(10), 2992-2999. Available At: https://turcomat.org/index.php/turkbilmat/article/view/4949

Elnaim, B. M. (2013). **Cybercrime in Kingdom of Saudi Arabia: The threat today and the expected future.** Information and Knowledge Management, 3(12),14-19. Available At: https://cutt.us/3zEky

Krejcie, R. V. and Morgan, D. W. (1970). **Determining Sample Size for Research Activities.** Educational and Psychological Measurement,30, 607- 610.

Zayid, E. I. M. and Farah, N. A. A. (2017). **A study on cybercrime awareness test in Saudi Arabia - Alnamas region.** International Conference on Anti-Cyber Crimes (ICACC), 199-202. Available At: https://0o10ayv69-y-https-ieeexplore-ieee-org.kau.proxy.deepknowledge.io/document/7905290/authors#authors

"The Extent of Postgraduate sStudents' Awareness on Combating Cybercrimes in the Light of the Saudi Vision 2030: A survey study in the Faculty of Arts and Humanities at King Abdulaziz university"

Abstract:

The study aimed to identify the extent of awareness of the Saudi cybercrime-fighting system in light of the digital transformation within the vision of 2030 among male and female graduate students at the College of Arts and Humanities at King Abdulaziz University, in terms of knowing the extent of their awareness of the cybercrime mentioned in the system, and monitoring the extent of their awareness of the reporting tools Information crimes in Saudi Arabia, clarifying the reasons for weak awareness of the system, and revealing ways to combat and prevent information crimes in light of digital transformation in line with Vision 2030, according to their point of view. The study relied on the descriptive survey method through the questionnaire data collection tool. The study sample consisted of (317) male and female students. The study reached several results, the most important of which are: that the level of awareness of information crimes mentioned in the Saudi cybercrime control system reached a high degree among the study sample, with a mean of (2.79). The study revealed the reasons for the poor awareness of the Saudi cybercrime control system according to the viewpoint of the study sample members, and the most impactful reason is the lack of community members' interest in the cybercrime fight system by looking at it and knowing how important it is. Digital transformation in line with Vision 2030 according to the viewpoint of the study sample members, the most important of which is the development of secure software and strong operating systems that limit electronic intrusions. The study, with a mean of (2.14). One of the most important recommendations of the study recommends the need to continuously develop and update the Saudi cybercrime control system to keep pace with all types of cybercrime and its emerging and emerging patterns.

Keywords: Cybercrime, Anti-Cybercrime Law, Digital transformation, Information Security, Vision 2030.