مجلـــــة العلـــــوم التربـــــوية والدراســـــات الإنســـــانيــــة
ISSN: 2709-0302 (online)

Humanities and Educational Sciences Journal
ISSN: 2617-5908 (print)

استراتيجية مقترحة لتوعية المرأة بنظام مكافحة الجرائم المعلوماتية في المجتمع السعودي

"دراسة وصفيه مطبقة على عينة من السيدات في مدينة الرياض"(*)

د/ عواطف يحيى القحطاني
أستاذ خدمة الجماعة المساعد
كلية الخدمة الاجتماعية
جامعة الأميرة نوره بنت عبد الرحمن
ayalqahtani@pnu.edu.sa

*) تاريخ تسليم البحث 27/11/2022 تاريخ قبوله للنشر 1/12/2022
*) موقع المجلة: http://hesj.org/ojs/index.php/hesj/index

استراتيجية مقترحة لتوعية المرأة بنظام مكافحة الجرائم المعلوماتية في المجتمع السعودي

"دراسة وصفيه مطبقة على عينة من السيدات في مدينة الرياض"

د/ عواطف يحيى القحطاني
أستاذ خدمة الجماعة المساعد
كلية الخدمة الاجتماعية
جامعة الأميرة نوره بنت عبد الرحمن

ملخص الدراسة

هدفت الدراسة الى التوصل الى استراتيجية مقترحة لتوعية المرأة السعودية بنظام مكافحة الجرائم المعلوماتية من خلال التعرف على مستوى الوعي لديها بأنواع الجرائم المعلوماتية التي يمكن ان تتعرض لها ووعيها بنظام مكافحة تلك الجرائم في المملكة العربية السعودية، بالإضافة إلى آرائها حول استراتيجيات المكافحة، حيث اتبعت الدراسة منهج المسح الاجتماعي على عينة من النساء السعوديات بلغت (449) سيدة سعودية، وتوصلت الدراسة الى ان هناك وعي مرتفع لدى المرأة السعودية بأنواع الجرائم المعلوماتية المختلفة التي يمكن ان تتعرض لها، وان لديها وعي بالعقوبات الجنائية وفقا لنظام مكافحة الجرائم المعلوماتية السعودي، بالإضافة للتأييد المرتفع للاستراتيجيات المختلفة التي يمكن ان تزيد من وعي المرأة السعودية بنظام مكافحة الجرائم المعلوماتية التي يمكن ان تتعرض لها، وخرجت الدراسة بمجموعة من التوصيات الموجهة للمرآة السعودية كوقاية ذاتية لعدم تعرضها لهذه النوعية من الجرائم، وتوصيات موجهة الى الجمعيات الأهلية المتخصصة في مجال المرأة لكي يكون لها دور في هذه التوعية، بالإضافة الى مجموعة توصيات مقترحة للجهات الرسمية المختلفة تشمل وزارة الاتصالات والداخلية والتعليم لزيادة وعي المرأة السعودية بالجرائم المعلوماتية وحمايتها منها.

الكلمات المفتاحية: الاستراتيجية – التوعية – الجرائم المعلوماتية – المرأة السعودية.

A Proposed Strategy to Educate Saudi Women about the System of Combating Information Crimes in Saudi Society: A Descriptive and Applied Study on a Sample of Women in Ryiadh

Dr. Awatif Yahya Al Qahtani
Assistant Professor of Social Service College of Social Service Princess Nora Bint Abdulrahman University

Abstract:

The study aims to come up with a proposed strategy to educate Saudi women about the system of combating information crimes by identifying their level of awareness of the types of information crimes that they may be exposed to and their awareness of the system of combating those crimes in the Kingdom of Saudi Arabia. Moreover, the study aims at exploring their views on the strategy of combating. The study has followed the social survey approach on a random sample of Saudi women that includes 449 Saudi women. The study has concluded that there is a high awareness among Saudi women of the different types of information crimes that they may be exposed to. They have awareness of criminal penalties according to the Saudi system of combating information crimes, in addition to the high support for different strategies which increase Saudi women's awareness of the system of combating information crimes that they may be exposed to. The study has come out with a set of recommendations addressing the Saudi women as self-prevention for not being subjected to this type of crime. The recommendations have addressed the civil societies specialized in the field of women in order to have a role in this awareness. Moreover, set of suggested recommendations have been given to the various official instiutions including: The ministry of communications, interior and education to increase Saudi women's awareness of combating information crimes.

Keywords: Strategy, Awareness, Information Crimes, Saudi Women.

المقدمة:

يعيش العالم المعاصر أزهى عصوره من خلال الاعتماد على ما تقدمة الثورة المعلوماتية مما ينعكس على جميع وجوه النشاط الإنساني وعلى العلاقات الدولية في جميع المجالات من خلال توحيد العالم إلكترونيًا عبر شبكات معلوماتية عملاقه تتدفق خلالها المعلومات من بلد لآخر ومن الطبيعي أن يتعرض مجتمع الإنترنت في ظل هذه الثورة المعلوماتية لبعض المخاطر والتهديدات ومنها الجرائم المعلوماتية حيث ترتبط هذه الجرائم بمدى اعتماد المجتمع بمؤسساته المختلفة الخاصة والعامة على الأنظمة المعلوماتية في إنجاز أعمالها كما أن هذه الجرائم تشكل تهديدا مباشرا لأكثر المرافق العامة والمصالح الخاصة، وتمثل عدوانا على حقوق الأفراد فيما يخص خصوصياتهم الاقتصادية والاجتماعية، كما أدى ظهور هذه الجرائم إلي إيجاد تحديات كثيره في مواجهة النظام القانوني القائم في العديد من الدول وخاصه في قانون العقوبات لذلك كان من الضروري حماية مستخدمي الأجهزة الذكية من التعرض لهذه الجرائم من خلال توعيتهم بأنواع الجرائم المعلوماتية وكيفيه التصدي لها وسن القوانين والتشريعات اللازمة لمكافحة الجرائم المعلوماتية نظراً لما تسببه من خسائر مادية ومعنوية كبيرة ولما لها تأثير على الأمن الاجتماعي لدى الدول والأفراد.

كما ان ارتفاع مستوى الجريمة المعلوماتية بشكل كبير أصبح يشكل تهديداً كبيراً في المجتمع الرقمي؛ حيث ازداد انتشار هذا النوع من الجرائم بسرعة كبيرة إلى درجة أنها أصبحت تمثل جزءًا من الجرائم التي من الممكن أن يتعرض لها الأفراد يومياً في حياتهم، فعلى سبيل المثال، عالمياً تضرر نحو(978) مليون شخص في (20) بلد بسبب جرائم المعلومات في عام (2017)، كما أن حوالي (172) مليار دولار فقدوا بسبب هذه الجرائم، وجاءت دولة الصين في الترتيب الأول بين ضحايا هذه الجرائم حول العالم بعدد (353) ضحية، وعربياً، أظهرت التقارير أن وحدة مكافحة الجرائم الإلكترونية في الأردن تعاملت خلال عام 2017م مع أكثر من 4200 قضية كان 80% من ضحاياها نساء، وخليجياً، كشفت الإحصاءات عن أن 67% من مستخدمي الإنترنت في دولة الإمارات المتحدة يعانون من الجرائم السيبرانية أما محلياً، فتشير الإحصائيات إلى أن نسبة تعرض سكان المملكة العربية السعودية للتهديدات الإلكترونية بلغ ما نسبته 39% (الجاسر، 2021).

كما أثبتت كثير من الدراسات أن المرأة هي أكثر شرائح المجتمع عرضة للوقوع ضحايا للجرائم المعلوماتية Kasuhik, 2014; Boskovic, 2022; Bhat, & Ahmad, (2022).، الأمر الذي جعلها غير آمنة بسبب ارتفاع نسبة الجرائم الممارسة ضدها في هذا العالم الافتراضي، فعلى سبيل المثال، يذكر ويست (West, 2014) أنه على الرغم من انتشار الجرائم الممارسة ضد المرأة عموماً، إلا أن هنالك العديد من الجوانب التي تجعل جرائم المعلومات الممارسة ضد النساء تحديداً متميزة عن باقي الجرائم التي تتعرض لها المرأة في حياتها اليومية، ولعل أهم هذه الجوانب وأولها صعوبة الكشف عن هوية المجرم مما يؤدي في أوقات كثيرة إلى إفلاته من العقوبة القانونية، إضافة إلى سهولة ارتكاب جرائم المعلومات كونها تتطلب القليل من المعرفة التقنية والتكلفة للقيام بها، كما أن القدرة على الاتصال السيبراني بأي شخص كان من أي مكان في العالم يوسع من مجموع

الضحايا ،المحتملين، وقد يكون سبباً في تعرض المرأة للجريمة الإلكترونية، مما يجعلنا نحاول التطرق إلى أهمية التوعية للمرأة بأنواع هذه الجرائم، من خلال استراتيجية مقترحة لتوعيتها بنظام مكافحة الجرائم المعلوماتية التي قد تتعرض لها أثناء تعاملاتها الرقمية اليومية.

مشكلة الدراسة:

شهد الوطن العربي منذ منتصف تسعينيات القرن الماضي ثورة إعلامية واتصالية هائلة تمثلت في ظهور الإنترنت، بالإضافة لظهور وسائل التواصل الاجتماعي (الميديا الاجتماعية) كأحد روافد تلك الثورة التكنولوجية، وكانت دول الوطن العربي من أكثر المتأثرين بهذا التطور التكنولوجي في الاتصال بسبب ثورة الأقمار الصناعية وتعدد قنواتها التلفزيونية حتى وجدت الدول العربية نفسها أمام العديد من وسائل التواصل الجديدة التي كانت لها مزايا وسلبيات، وقد أدت وسائل التواصل الاجتماعي لتحولات اجتماعية عميقة في الدول العربية عامة والمملكة العربية السعودية خاصة وساهم التقدم الهائل الذي اضحى واضحًا في المجال التكنولوجي، والزيادة المضطردة في عدد مستخدمي التكنولوجيا والأجهزة الحديثة في ظهور فئة جديدة من الإجرام، مرتبطة بالتكنولوجيا، ومنها الجرائم المعلوماتية (البطاشي، 2021: 55).

ويلاحظ أن هذه الجرائم في تزايد مستمر بين الشباب والفتيات في المجتمع السعودي، خاصة أن لهذا النوع من الجرائم العديد من الآثار الاجتماعية والنفسية على مستوى الأفراد والجماعات، الأمر الذي يتطلب سرعة مواجهة ومكافحة هذه الجريمة والبحث عن أسباب ظهورها وانتشارها ووضع برامج وقائية لها (الحميدي، 2011: 89).

وقد استعرض (البداينه، 2014) عدة أسباب لظهور الجريمة المعلوماتية وانتشارها منها: سهولة استهداف الضحايا، سرعة التنفيذ وقلة التكلفة، ضعف الرقابة وصعوبة ملاحقة الجناة، إلخ. ولعل أهم أسباب انتشار الجريمة المعلوماتية يعزى إلى قلة الوعي بنظام مكافحة الجرائم المعلوماتية والعقوبات المترتبة على هذه الجرائم. كما أكد (الهيف والعنزي، 2018) على ضرورة التوعية بالجرائم المعلوماتية عن طريق النشر المكثف لتلك البرامج من خلال وسائل الإعلام.

كما أكد (الخالدي، 2020) على ضرورة رفع درجة الوعي الاجتماعي لدى المرأة واعطائها مزيدا من الدعم والمساندة لكونها تمثل العنصر الأساسي للإبلاغ عن أي ظاهره سلبية داخل الاسرة لا سيما ظاهرة الابتزاز الإلكتروني.

وتوصل (الجعبري، عمرو) في عام 2020 إلى أن المعرفة بقانون الجرائم والعقوبات المترتبة عليها سيكون رادعا للعديد من الأفراد من ارتكاب أي سلوك إلكتروني مخالف للقانون.

وتعد المملكة العربية السعودية من الدول التي لم تغفل عن توفير الأمن الرقمي؛ فقامت بإصدار النظام الذي يحد من الجرائم المعلوماتية ويسهم في تحقيق الأمن المعلوماتي وهو نظام مكافحة الجرائم المعلوماتية وسيتم في هذه الدراسة التعرف على أنواع الجرائم المعلوماتية التي تتعرض لها المرأة في المجتمع السعودي والتوصل إلى استراتيجية

مناسبه لتوعية المرآه بنظام مكافحة الجرائم المعلوماتية، ولأهمية موضوع الدراسة وهو الجرائم المعلوماتية وخصوصاً ضد المرأة والوعي بها وكيفية التصدي لها ، والخروج باستراتيجيات مقترحة لتوعية المرأة بالجرائم المعلوماتية وكيفية التصدي لها فإن الدراسة الحالية تحاول الإجابة عن التساؤلات الآتية:

- ما مستوى وعي المرأة السعودية بأنواع الجرائم المعلوماتية التي يمكن أن تتعرض لها المرأة؟
- ما مستوى وعي المرأة السعودية بنظام مكافحة الجرائم المعلوماتية؟
- ما الاستراتيجيات المقترحة لتوعية المرأة بنظام مكافحة الجرائم المعلوماتية؟

الأهداف:

تهدف الدراسة للتوصل إلى استراتيجية مقترحة لتوعية المرأة بنظام مكافحة الجرائم المعلوماتية في المجتمع السعودي من خلال:

1- التعرف على مستوى وعي المرأة السعودية بأنواع الجرائم المعلوماتية التي يمكن أن تتعرض لها المرأة.

2- التعرف على مستوى وعي المرأة السعودية بنظام مكافحة الجرائم المعلوماتية.

3- التوصل إلى استراتيجية مقترحة لتوعية المرأة ل بنظام مكافحة الجرائم المعلوماتية.

الأهمية:

الأهمية النظرية:

- يتناول البحث استراتيجية مقترحة لتوعية المرأة بنظام مكافحة الجرائم المعلوماتية في المجتمع السعودي الذي يعد من الموضوعات الهامة التي تمس المرأة وما تتعرض له في عصر المعلومات والمعرفة من جرائم قد لا تكون واضحة للكافة، لذا يسلط البحث الضوء على أنواع هذه الجرائم كما يسلط الضوء على نظام مكافحة الجرائم المعلوماتية بالمملكة العربية السعودية وتصديه لهذه الجرائم المعلوماتية، وعرض ما توصلت إليه الدراسات السابقة لهذا البحث بهذا الخصوص في مجالات مختلفة ولم تكتفي بمجالات الخدمة الاجتماعية بل شمل القانون وعلم النفس وعلم الاجتماع وعلم المعلومات، والعلوم المختلفة.
- ندرة البحوث والدراسات التي تناولت الاستراتيجيات المقترحة لزيادة وعي المرأة السعودية بنظام مكافحة الجرائم المعلوماتية من استراتيجيات متنوعة تبدأ من ذاتها مروراً بمؤسسات المجتمع المدني ومؤسسات الدولة.

الأهمية التطبيقية:

- الاستفادة من نتائج الدراسة الحالية للتعرف على واقع معرفة المرأة السعودية بمختلف مستوياتها التعليمية والمراحل السنية المختلفة بالجرائم المعلوماتية المختلفة ومدى وجود قصور في هذه المعرفة من عدمه.
- رفع الوعي المجتمعي لدى المرأة السعودية المشاركة في الدراسة ومن حولها في تسليط الضوء على الجرائم المعلوماتية وأنواعها ونظام مكافحة هذه الجرائم في المملكة والعقوبات الخاصة بها.
- وضع الاستراتيجيات المقترحة تحت تصرف متخذي القرار وذوي العلاقة للاستفادة منها في زيادة الوعي بالجرائم المعلوماتية لدى المرأة السعودية.

حدود الدراسة:

- **الحدود المكانية والبشرية:** السيدات السعوديات في مدينة الرياض، وتم اختيار مدينة الرياض لإنها العاصمة وأكثر مدن المملكة من حيث عدد السكان وتشهد تطورًا ملحوظًا.
- **الحدود الزمنية:** فترة جمع البيانات من 2022/10/20م حتى 2022/10/31م.
- **الحدود الموضوعية:** مستوى وعي المرأة السعودية بأنواع الجرائم المعلوماتية التي يمكن أن تتعرض لها، ومستوى الوعي بنظام مكافحة الجرائم المعلوماتية بالمملكة، والخروج باستراتيجيات مقترحة لتوعية المرأة بنظام مكافحة الجرائم المعلوماتية ضدها.

مصطلحات الدراسة:

- **الاستراتيجية:**

تناولت ميرفت شمروخ الاستراتيجية بأنها الكيفية التي يتم من خلالها حشد جميع الإمكانيات البشرية والمادية للدولة لجميع مكوناتها من أجل تحقيق غايات وأهداف كبرى ومن خلال خطط عامة أو برامج مدروسة تتسم بالشمول والعمق الزمني (شمروخ ،2017: 452).

ويمكن تعريفها إجرائياً: بأنها الأساليب المختلفة التي يمكن استخدامها لمواجهة تهديدات ومشاكل الجرائم المعلوماتية التي قد تواجه المرأة السعودية لحمايتها من هذه التهديدات.

- **التوعية:**

تُعرف التوعية لغة بأنها: مأخوذة من الوعي ويقصد به عدة معاني منها حفظ القلب للشيء، والفهم وسلامة الادراك (أنيس واخرون، 2014: 1044).

كما يمكن تعريفها: "بأنها اثارة الوعي تجاه قضية معينه بهدف تغيير الأنماط السلوكية أو تغيير وتعديل اتجاهات الراي العام تجاه هذه القضايا من اتجاهات سلبيه الى اتجاهات ايجابيه أو من تعاطف الى رفض ومواجهة بحسب طبيعة القضية وتأثيرها في المجتمع" (عجوة، 2014: 39-40).

ويمكن تعريفها إجرائياً: بأنها عملية مستمرة ومتكاملة تهدف الى اكساب المرأة السعودية وعياً حول الجرائم المعلوماتية وتبصيرها بالجوانب المختلفة المرتبطة بها.

- **الجريمة المعلوماتية:**

عرفها تيجيني (2020: 117) بأنها كل نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي/ الجوالات الذكية بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي، وينشأ عنه خسارة تلحق بالمجني عليه أو مكسب يحققه الفاعل، وتناولت الهيف (2022: 49) الجريمة المعلوماتية بأنّها الممارسات التي تُوقَع ضدّ فرد أو مجموعةٍ مع توفّر باعثٍ إجراميّ بهدفِ التَّسبُّبِ بالأذى لسمعة الضحيّة عمداً، أو إلحاق الضَّرر النفسيّ والبدنيّ به سواءً أكان ذلك بأسلوبٍ مباشر أو غير مباشر بالاستعانة بشبكات الاتّصال الحديثة كالإنترنت وما تتبعها من

أدوات كالبريد الإلكتروني وغرف المحادثة، والهواتف المحمولة وما تتبعها من أدوات كرسائل الوسائط المتعدّدة.

ويمكن تعريفها إجرائياً: هي أي ممارسة تقع ضد المرأة مع توفر شق إجرامي يستهدف سمعتها أو إلحاق الضرر النفسي أو البدني بها بأسلوب مباشر أو غير مباشراً من خلال استخدام وسائل الاتصال الرقمية الحديثة، وينشأ عنها خسارة تلحق بالمرأة سواء مادي أو معنوي.

نظام مكافحة الجرائم المعلوماتية:

هو نظام مكافحة جرائم المعلوماتية صدر بمرسوم مرسوم ملكي رقم م/17 بتاريخ 1428/3/8هـ، ويهدف إلى الحد من وقوع الجرائم المعلوماتية، وذلك بتحديد هذه الجرائم والعقوبات المقررة لكل منها، وبما يؤدي للمساعدة على تحقيق الأمن المعلوماتي، وحفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية، وحماية المصلحة العامة، والأخلاق، والآداب العامة، والاقتصاد الوطني (هيئة الخبراء بمجلس الوزراء، 2022).

المنطلق النظري للدراسة:

تطور جرائم المعلومات:

أن تطور الجريمة المعلوماتية لم يكن بمحض الصدفة، فقد مر هذا النوع من الجرائم بعدد من التطورات فيذكر كل من دونير وماركوم وجينينغز وهيجينز وبانفيلد (Donner, Marcum, Jennings, Higgins,& Banfield 2014 أنه من الممكن تقسيم المراحل التي مرت بها الجرائم المعلوماتية إلى ثلاث مراحل رئيسة، فيتضمن الجيل الأول من الجريمة المعلوماتية الخاصة بالسلوك المنحرف التي تتمثل في الاستخدام غير القانوني لشبكة الإنترنت والتي كانت موجودة قبل إنشاء أجهزة الكمبيوتر، لكن ومع التطورات التكنولوجية توفرت للمجرمين مساحة جديدة لاكتشاف طرق تساعدهم على ارتكاب هذه الجرائم، في حين يعد الجيل الثاني للجريمة المعلوماتية جريمة هجينة؛ حيث إن هذا النوع من الجرائم كان موجوداً بالفعل في السابق ولكن ازداد ارتكابه وتم تكييفه من خلال استخدام الإنترنت، وتعد القرصنة أحد أكثر الأشكال الشائعة للجرائم المعلوماتية في هذه المرحلة؛ فهي تحاكي سرقة خطوط الهاتف من شركات الاتصالات الأرضية قديماً واستخدامها لإجراء المكالمات مجاناً، كما أن نشر الصور الإباحية أو التحرش الجنسي تعد أيضاً أمثلة على هذه المرحلة، فجرائم التحرش كانت موجودة قبل إنشاء الإنترنت ولكن – ومع التطور التقني – استطاع المجرمون أن يرتكبوها بطرق مختلفة – وغالباً ما تكون طرق يصعب اكتشافها مقارنة بالتحرش التقليدي، وأخيراً تعتمد الجرائم المعلوماتية في المرحلة الثالثة على الإنترنت كلياً؛ حيث إن الجرائم في هذا الجيل لم يكن من الممكن أن يكون لها وجوداً إن لم يكن للإنترنت وجود، حيث تعد شبكة الإنترنت المكان الوحيد الذي يمكن أن تحدث فيه هذه الجرائم، ويعد نشر البرامج الضارة والفيروسات أبرز مثال على هذا الجيل من الجرائم المعلوماتية.

وبناءً على هذا التطور في الجرائم المعلوماتية، ظهرت أشكال متعددة من الممارسات الغير مشروعة عبر الإنترنت والتي أصبحت تعد مشكلة حقيقة للنظام الجنائي، فالاستيلاء على بطاقة ائتمان شخص أو أي من

معلوماته الشخصية لا يتطلب سرقتها أو الحصول عليها بطريقة فعلية وبشكل مادي؛ حيث إن كل هذه المعلومات أصبح من الممكن الوصول إليها عبر الإنترنت والاستيلاء عليها افتراضياً واستخدامها لأغراض احتيالية، كما أن الجرائم الجنسية مثل إنتاج المواد الإباحية أو الاتجار بالبشر بل وحتى البغاء أصبحت ممارستها أسهل مع وجود الإنترنت، علاوة على ذلك، سهل وجود الإنترنت الحصول مجاناً على مواد محمية بحقوق الطباعة والنشر مثل الأغاني والأفلام والبرامج والتي يتم تحميلها بشكل غير قانوني عبر شبكة الإنترنت (الجاسر، 2021: 203).

صور الجرائم المعلوماتية:

ينقسم الباحثون في تلك الجرائم الى فئات متعددة تختلف حسب الأساس والمعيار الذي يستند إليه التقسيم المعني، فبعضهم يقسمها إلى جرائم ترتكب على نظم المعلومات، وأخرى ترتكب بواسطته، وبعضهم يصنفها ضمن فئات الأسلوب المتبع في الجريمة، وآخرون يستندون إلى الباعث أو الدافع لارتكاب الجريمة، وغيرهم يؤسس تقسيمه على تعدد محل الاعتداء، وكذا تعدد الحق المعتدى عليه فتوزع الجرائم المعلوماتية وفق هذا التقسيم إلى جرائم تقع على الأموال بواسطة النظم المعلوماتية وتلك التي تقع على الحياة الخاصة، فهناك الجرائم الواقعة على ذات المعلومات, كجرائم الإتلاف والتشويه للبيانات والمعلومات وبرامج الحاسب بما في ذلك استخدام وسيلة (الفيروسات) التقنية، وهناك الجرائم الواقعة على ما تمثله المعطيات آليا من أموال أو أصول؛ كجرائم غش الحاسب التي تستهدف الحصول على المال، أو جرائم الاتجار بالمعطيات, وجرائم التحوير والتلاعب في المعطيات المخزنة داخل نظم المعلومات واستخدامها (تزوير المستندات المعالجة آليا واستخدامها)، كما أن هناك الجرائم الماسة بالمعطيات الشخصية أو البيانات المتصلة بالحياة الخاصة وتشمل جرائم الاعتداء على المعطيات السرية أو المحمية وجرائم الاعتداء على البيانات الشخصية المتصلة بالحياة الخاصة، وبإمعان النظر في هذه الطوائف، نجد أن الحدود بينها ليست قاطعة ومانعة، فالتداخل حاصل ومحقق، إذ إن الاعتداء على معطيات الحاسب بالنظر لقيمتها الذاتية أو ما تمثله، هو في ذات الوقت اعتداء على أمن المعطيات، لكن الغرض المباشر المحرك للاعتداء انصب على قيمتها أو ما تمثله (فكري، 2014: 159-160).

وقد قسم بيرغ وجنغير Bergh & Junger (2018) الجرائم المعلوماتية إلى:

- جرائم التسوق عبر الإنترنت والتي تتسم بعدم القدرة على فحص البضائع قبل شرائها أو عدم وجود الاتصال المباشر بين الأطراف المعنية في عملية البيع والشراء.
- الاحتيال المصرفي عبر الإنترنت والذي يحدث عندما يتمكن المحتال من الوصول إلى الحساب البنكي لأحد الأفراد على الإنترنت وتحويل الأموال منه.
- أنواع الاحتيال الأخرى والتي تشمل طلب رسوم مقدمة عن طريق إيهام الضحية بأنه سيحصل على حصة كبيرة من مبلغ مالي في مقابل دفع مبلغ صغير مقدماً، وتشمل أيضاً سرقة هوية شخص آخر لتحقيق مكاسب مالية أو مزايا أو إيقاع الضرر بهذا الشخص.
- التنمر السيبراني وهو يحاكي التنمر في الواقع لكنه يعتمد على تقنيات الإنترنت لارتكابه.

- البرامج الضارة وهو مصطلح يستخدم للإشارة إلى مجموعة متنوعة من البرمجيات التي من شأنها الإضرار بجهاز الضحية مثل الفيروسات.
- القرصنة أو اختراق الكمبيوتر: فالمخترق هو الشخص الذي يسعى إلى خرق الدفاعات واستغلال نقاط الضعف في نظام الكمبيوتر من أجل الدخول إلى نظام الضحية.

كما قام كل من هالدير وجايشانكار Halder & Karuppannan (2009) بتحديد عشر أنماط أساسية من الجرائم المعلوماتية التي قد تتعرض لها المرأة عبر الإنترنت، وهي:

- التحرش عبر الرسائل الإلكترونية حيث يستهدف تخويف المرأة عن طريق إرسال رسائل مسيئة لها عبر وسائل التواصل الإلكترونية المختلفة.
- التعقب السيبراني وتنطوي هذه الجريمة على استخدام الإنترنت لمضايقة شخص ما على وجه الخصوص، ويشمل نشر الاتهامات الكاذبة عنه والتهديدات والتنمر السيبراني وغيرها.
- الاستغلال الجنسي عبر الإنترنت حيث تقع المرأة ضحية للاستغلال الجنسي من التواصل عبر الإنترنت.
- القرصنة الإلكترونية أي استخدام غير مصرح به للإنترنت والذي يحاول المخترق من خلاله إلى الوصول إلى أي نظام.
- تشهير المرأة عبر الإنترنت وهو نشر مواد تشهيرية للمرأة بمساعدة أجهزة الكمبيوتر أو الإنترنت.
- التعديل وهو استخدام أدوات معالجة الصور لتعديل صور المرأة للتشهير بها.
- المعاكسات الإلكترونية وهو استخدام الإنترنت لإرسال رسائل غزل استفزازية للمرأة.

ومن خلال مراجعة الأدبيات السابقة، يتضح لنا عدم وجود أي تقسيم لأنماط الجرائم السيبرانية التي يتم التعرض لها عبر وسائل الإعلام الجديد، وخاصة تلك الممارسة ضد المرأة ومن ثم تسعى الدراسة الحالية إلى التعرف على أبرز أنماط الجرائم السيبرانية الممارسة ضد المرأة عبر وسائل الإعلام الجديد.

النتائج السلبية لوقوع المرأة ضحية للجرائم المعلوماتية:

تتعد الآثار السلبية للجرائم المعلوماتية التي تقع ضحيتها المرأة بين كونها آثار نفسية واجتماعية وجسدية واقتصادية، فقد ذكر west (204) أن أكثر هذه التأثيرات هي التأثيرات النفسية والتي تتضمن الشعور المفرط بالقلق، والرغبة في إيذاء الذات، وظهور الميول الانتحارية والتي تقود في بعض الأحيان إلى محاولة الانتحار الفعلي، كما يمكن للجرائم المعلوماتية ضد المرأة أن يكون لها آثاراً اقتصادية خطيرة أيضاً، فكثير من السيدات يفقدن وظائفهن بسبب المواد المسيئة التي تم نشرها عنهن عبر الإنترنت، ومع محو الأشياء من الإنترنت بشكل تام، أصبح تأثير الصور الإباحية والتشهير بالمرأة عبره ذا تأثير دائم، الأمر الذي قد يمنعهن من العمل في وظائف جديدة أو التقدم في وظائفهن الحالية، كما يمكن أن يتزامن العنف السيبراني مع العنف الجسدي ضد المرأة أو يؤدي إلى تفاقمه أو حتى يؤدي إلى حدوثه، كما يمكن أن تكون العواقب الاجتماعية للجرائم المعلوماتية ضد المرأة شديدة للغاية، فقد تتأثر عائلتها بأسرها بآثارها، كما أن التأثير الاجتماعي قد يشمل العزلة عن الأصدقاء والعائلة، وفي

حالات مختلفة قد تمتثل المرأة لتهديدات القائم بالجريمة المعلوماتية لتفادي مثل هذه الآثار السلبية عليها وعلى المحيطين بها، مما أكد على أهمية معرفة حقوق المرأة عند تعرضها لهذه الجرائم وأهمية وعيها بأنظمة مكافحة الجرائم المعلوماتية بالمملكة العربية السعودية، وأن الجريمة المعلوماتية التي قد تتعرض لها ما هي إلا جريمة كأي جريمة يعاقب عليها القانون ولا تسيئ إليها في شيء بل على مرتكبها، لذا يظهر دور التوعية والإعلام لتجنب هذه الآثار السلبية للجرائم المعلوماتية التي تتعرض لها المرأة للحد منها أو التقليل من ضررها.

نظرية الدراسة: نظرية الأنشطة الروتينية:

تقدم نظرية الأنشطة الروتينية تفسيرًا واضحًا لسبب حدوث الجرائم. وبالتحديد، تحاول توضيح سبب الجريمة التي تحدث في ظل بعض الظروف المحددة بدلًا من فهم الخصائص الإجرامية للجناة. وتم تطبيقها في الماضي على جرائم الاتصال المباشر وجرائم الملكية؛ وفي الوقت الحاضر فهي قابلة للتطبيق على أنواع أخرى كثيرة من السلوكيات المنحرفة، حيث تم استخدامها في تفسير التغيرات في اتجاهات وقت الجريمة، ولقد تم استخدامها بشكل تدريجي بشكل أكثر عمومية لتحديد مشكلات الجريمة وتعريفها ومنعها، ويقصد كوهين وفيلسون أحد مؤسسي هذه النظرية بمفهوم "الأنشطة الروتينية" أنه خلال الأنشطة اليومية والعادية للحياة، يضع الأفراد أنفسهم في مواقف تزيد أو تقلل من خطر تعرضهم للإيذاء الجنائي، كما تقدم النظرية تصورًا للجوانب الظرفية للجريمة من خلال الجمع بين الزمان والمكان كسبب حتمي للفهم الجنائي لأماكن الجريمة، فتركز على الجوانب الظرفية والمكانية الأمر الذي يجعل الجريمة سمة متأصلة في الأشخاص الذين يتم التفاعل معهم في المجتمع، والأماكن التي نسافر إليها، والأنشطة التي نشارك فيها، والتأثير على احتمالية وحدوث السلوك الإجرامي، فوجود الجاني الدافع والهدف المناسب وانعدام الرقابة لا يعني أن الجريمة أمر لا مفر منه. ولكن تؤكد النظرية بأن احتمال الجريمة يزيد أو ينقص بناءً على وجود هذه العناصر الثلاثة، وأهم فرضيات نظرية الاختيار العقلاني "أن الجريمة تحتاج إلى فرصة للقيام بها"، بمعنى أن الموقف الذي يجد الفاعل نفسه فيه يمكن أن يمنحه الفرصة لكي يقوم بالفعل الإجرامي. ولقد ترتب على هذه الفرضية فرضية أخرى أدت إلى ظهور نموذج النشاط الروتيني، وتذهب هذه الفرضية إلى القول "بأن التغيرات في أسلوب الحياة أو في الأنشطة الروتينية في الحياة تؤثر على طبيعة الفرص المتاحة لارتكاب الجريمة" (زايد، 2017: 190).

حيث تتطلب هذه النظرية وجود ثلاثة عناصر لحدوث جريمة بشكل عام وهي مجرم له نوايا إجرامية متحمس وله القدرة على التصرف وفقًا لهذه الميول الإجرامية، بالإضافة على الضحية المناسبة وأخيراً إلى غياب للمانع للجريمة أي الشخص الذي له القدرة على منع وقوع الجريمة؛ وعند تلاقى هذه العناصر الثلاثة في المكان والزمان لحدوث جريمة، حيث توفر هذه النظرية منظورًا كليًا للجريمة من حيث أنها تتوقع كيف تؤثر التغيرات في الظروف الاجتماعية والاقتصادية على معدل الجريمة والإيذاء بشكل عام، ويفترض فيلسون وكوهين أن الأنشطة الإجرامية هي "ظاهرة بنائية مهمة"، الأمر الذي يعني أن الانتهاكات ليست أحداثًا عشوائية ولا تافهة. ونتيجة لذلك؛ فإن روتين الأنشطة التي يشارك فيها الأشخاص على مدار حياتهم النهارية والليلية هو الذي يجعل بعض الأفراد أكثر

عرضة لأن يُنظر إليهم على أنهم أهداف مناسبة من قبل الجاني الذي يحسب ذلك عقلانيًا. لذلك؛ فإن الجريمة تعتمد على الفرص المتاحة إذا كان هناك هدف غير محمي، وكان هناك مكافآت كافية، فإن الجاني المتحمس يرتكب الجريمة (سليمان، 2022: 117).

تشرح النظرية الزيادة في عدد ضحايا الجرائم الإلكترونية من خلال تغيير الأنشطة اليومية للناس في حياتهم اليومية. مع ظهور الإنترنت، تغيرت طريقة تواصل الأشخاص أو تفاعلهم مع الآخرين في العلاقات والترفيه والأعمال وغير ذلك. بالإضافة إلى ذلك، فإن التغييرات في الأنشطة اليومية للأشخاص، مثل استخدام الإنترنت، والشبكات الاجتماعية، والفيسبوك، والبريد الإلكتروني، والمواقع الإلكترونية، وما إلى ذلك، تخلق فرصًا لحدوث الجرائم حيث تجتمع ثلاثة عوامل: الجناة المتحمسون، والأهداف المناسبة، وغياب الإشراف لأن هذه العوامل الثلاثة يجب أن تكون موجودة لحدوث الجريمة، وغياب أي من هذه العوامل كافٍ لمنع حدوثها بنجاح لإكمال ارتباط مباشر بحدوث الجريمة، وهذا التقارب يمكن أن يؤدي إلى زيادة كبيرة في الجريمة معدلات الجريمة، ولا يوجد تغيير في "الحالة البيئية" التي تحفز المجرمين، وبالتالي تؤثر على معدل الجريمة، والعناصر النظرية الرئيسية الثلاثة في العالم الافتراضي للجرائم الإلكترونية، وبالتالي تؤثر على معدل الجريمة، وعناصر النظرية الثلاثة الرئيسية في العالم الافتراضي للجريمة الإلكترونية، حيث إن الجاني المتحفز (قد يكون) والمستهدف المناسب (استهداف الهوية أو المال)، ولكن الحراسة القادرة كبرامج الحماية والبرامج المضادة للفيروسات (البدانية، 2014: 3).

باختصار؛ تقطع نظرية الأنشطة الروتينية شوطًا طويلاً في شرح أنواع مختلفة من الجرائم الإلكترونية لأن الجرائم لا تُرتكب إلا إذا كان من المحتمل حدوثها، ويعتقد الجاني أن الهدف مناسب وليس له أوصياء أكفاء، ويمكن لأنشطة الحياة اليومية أن تجعل الأشخاص في وضع يسمح لهم بأن يكونوا ضحية معرضة للجريمة.

الدراسات السابقة:

أولاً: الدراسات العربية

ألقت دراسة الدعجة (2014) الضوء على الاستراتيجيات الموضوعة والجهود المبذولة على الصعيدين الدولي والإقليمي والوطني وجهود الجامعة العربية، والخطط الموضوعة لتفادي تطور الجرائم المعلوماتية التي توازي سرعة تطورها سرعة تطور التكنولوجيا، مستخدمة المنهج الوصفي التحليلي ، والتي توصلت نتائجها إلى أن الجريمة المعلوماتية بحكم خاصيتها العابرة للحدود أوجبت على العالم الدخول في سياسات واستراتيجيات للحد من الآثار المترتبة عن هذه الجريمة، وأن الجهود المبذولة على المستوى المحلي والإقليمي العربي واستراتيجية المكافحة ما زالت لا تفي بالغرض خصوصاً مع تزايد الاستخدامات لشبكة الإنترنت والواقع الذي أصبحت تفرضه الحاجة، وأوصت أنه يجب على الدول العربية إتباع استراتيجية تتظافر بها جميع الجهود بمشاركة جميع الفعاليات على كافة المستويات والالتزام بالاتفاقيات العربية والدولية للتصدي أو للتخفيف من الآثار التي تنتجها مثل هذه الجرائم لا سيما الأخلاقية منها، وتطويع قواعد الاتفاقيات الدولية الخاصة بتسليم المجرمين وتفعيلها في كل دولة، لخصوصية الجرائم المعلوماتية من حيث صعوبة إثباتها ومتابعة مرتكبيها وسهولة إتلاف أدلتها كونها لا تترك أثر مادي في مسرح الجريمة.

تناولت دراسة غريب، والأمير (2017) الوعي لدى الفئة العمرية الشابة بنظام عقوبات الجرائم المعلوماتية السعودي، من خلال التعرف على مفهوم جرائم المعلومات وأشكالها بالإضافة ، ومدى وعي الشباب بعقوبات نظام الجرائم الإلكترونية، حيث أكدت نتائجها أن الغالبية العظمى من الشباب لديهم خوف من أن يكونوا أحد ضحايا الجرائم

الإلكترونية وان وسائل التواصل الاجتماعي هي المصدر الأول للتوعية بالجرائم الإلكترونية وان معرفة الأنظمة والعقوبات له دور أساسي في الحد من الممارسات السلبية للتقنية، كما أوصت الدراسة بضرورة تصميم وتنفيذ برامج وقائية للشباب للتوعية بعواقب الجرائم المعلوماتية وإقامة الندوات والمؤتمرات العلمية في مجال وقاية الشباب من مخاطر الجرائم المعلوماتية.

ومن خلال دراسة عبد الرازق (2017) للجرائم الإلكترونية ضد النساء والفتيات: المخاطر وطرق المواجهة، حاولت البحث عن مخاطر الجرائم الإلكترونية على النساء والفتيات، ومدى وعيهن بتلك المخاطر، وبحث سياسات وآليات تعامل المؤسسات التعليمية والاجتماعية والقانونية على مستويات الوقاية والحماية والملاحقة القانونية. والتعرف على: التأثيرات النفسية والاجتماعية إلي تقع على النساء والفتيات جراء تعرضهن لأشكال مختلفة من الجرائم الإلكترونية، ودور الأسرة في حماية الفتيات من الاستغلال والاعتداءات الإلكترونية، والتعرف على كيفية تعامل النساء والفتات عند تعرضهن للجرائم الإلكترونية. وطرق الوقاية والحماية، وكذلك الملاحقة القانونية لمرتكبي لتلك الجرائم، وأكدت نتائجها أن الوجه الآخر للإنترنت يكمن في مخاطر العنف الإلكتروني التي تؤثر على السلام والرخاء للجميع المنصوص عليها في ميثاق الأمم المتحدة: وأن من أكثر مظاهر العنف الإلكتروني شيوعاً على مستوى العالم ضد النساء والفتيات: المطاردة الملاحقة الإلكترونية، والابتزاز الإلكتروني. والتحرشات الجنسية الإلكترونية، والمراقبة والتجسس على أجهزة الحاسوب الهواتف الذكية والأجهزة اللوحية، والاستخدامات غير القانونية. باستخدام التكنولوجيا والإنترنت للصور ومقاطع الفيديو وتحريفها والتهديد بها والاتجار بالبشر للاستخدامات الجنسية غير المشروعة، وانتحال أسماء وشخصيات معروفة للإيقاع بالنساء والفتيات والطفلات. خاصة في غرف الدردشة ووسائط الإعلام الاجتماعي، وأن النساء والفتيات المتعرضات للعنف الإلكتروني تعاني من آثار شديدة الخطورة على المستوى الاجتماعي والنفسي. تتمثل في المشاكل العاطفية، وتفكك أسري والخوف المستمر من الملاحقة ومن مغادرة المنزل. واللوم، ولاتزال أسباب عدم إفصاح الفتيات والنساء وطلب المساعدة. عندما يتعرضن لأحد أشكال الجرائم الإلكترونية، نتيجة الخوف من الوصمة الاجتماعية من المحيط. فالأعراف الاجتماعية والتقاليد والتوقعات السائدة تبقى الحاضنة للعنف القائم على النوع الاجتماعي. وفي كثير من الأحيان تلام النساء والفتيات على أفعال لم يرتكبنها وغالباً ما تصل تلك القضايا للجهات الرسمية في المراحل الأخيرة من الابتزاز الذي يفوق قدرات الضحية على الاستجابة أو التحمل.

كما هدفت دراسة الهيف، العنزي (2018) التعرف على الجرائم المعلوماتية أنواعها وخطورتها، من خلال التعريف بمستوى وعي طالبات الجامعة بأنواع الجرائم المعلوماتية، ومدى خطورة الجرائم المعلوماتية، فضلاً عن التعرف على شكل ومضمون ومصادر الجرائم المعلوماتية، وطرق الوقاية منها، متبعة الدراسة المنهج الوصفي على عينة من طالبات قسم المكتبات والمعلومات في جامعة الأميرة نورة (238) طالبة، وتوصلت الدراسة إلى وجود دراية بوجود جرائم معلوماتية ووجود نظام لمكافحتها، وأن الشهرة والرغبة في تسليط الضوء هي سبب ودافع الجريمة الإلكترونية، وأوصت الدراسة بالنشر المكثف لبرامج التوعية للوقاية من الجرائم الإلكترونية، وأن تكون وسائل الإعلام هي المسؤولة عن التوعية بالجرائم المعلوماتية، بالإضافة إلى بأن الوعي الديني والأخلاقي من أهم العناصر التي تساعد في عدم الوقوع في الجرائم المعلوماتية.

وأكدت الجاسر (2021) في دراستها التي حاولت التعرف على مدى انتشار الجرائم السيبرانية الممارسة ضد المرأة السعودية عبر وسائل الإعلام الجديد، وعلى أنماط هذا النوع من الجرائم، مستعينة بالمسح الاجتماعي؛ حيث أكدت أن جرائم الاختراق السيبراني تصدرت قائمة أنماط الجرائم السيبرانية الممارسة ضد المرأة السعودية عبر وسائل الإعلام الجديد، واتخذت الجرائم الجنسية المرتبة الثانية، تلا ذلك الجرائم المالية، ثم جرائم تشويه السمعة، وجاءت سرقة المعلومات الشخصية في

المرتبة الأخيرة، وأوصت بالتوعية بالقوانين والتشريعات المتعلق بالجرائم السيبرانية عبر وسائل الإعلام الجديد والعقوبات التي تقع على مرتكبيها وتفعيل دور مؤسسات المجتمع المحلي في مجال التوعية المجتمعية المتعلقة بهاء ، وضرورة عقد ورش عمل واللقاءات للتوعية بأخطار الجرائم السيبرانية والتعريف بالعوامل الشخصية التي تسهل الوقوع كضحية لمثل هذه الجرائم- خاصةً.

كما قدم الزين (2021) دراسة بعنوان "الجرائم الإلكترونية ومستوى الوعي بخطورتها: دراسة ميدانية على عينة من الشباب الجامعي الأردني" حيث حاولت التعرف على الجرائم الإلكترونية ومستوى الوعي بخطورتها من وجهة نظر الشباب الجامعي الأردني في جامعة البلقاء التطبيقية كلية الأميرة رحمة الجامعية، والتعرف على عادات وأنماط استخدام الإنترنت لدى الشباب، مستخدمة المنهج الوصفي ومنهج المسح الاجتماعي بأسلوب العينة، وتكونت عينة الدراسة من (212) طالب وطالبة، حيث كشفت نتائجها أن معدل تعرض الطلبة للجرائم الإلكترونية جاء بمستوى منخفض، كما بينت نتائج الدراسة أن 39.15% يقضون من ساعتين إلى أقل من أربع ساعات على الإنترنت، أما أكثر المواقع استخداما فهو الفيس بوك بنسبة 49.06%، و43.40% يدخلون للمواقع بهدف الترفيه والتسلية، أما مستوى الوعي بالجرائم الإلكترونية فقد جاء مرتفعا، وأوصت الدراسة بضرورة توعية الطلبة بأهمية استثمار وقتهم عند استخدام الإنترنت لتطوير مهاراتهم، تفعيل النشاطات الرياضية، والثقافية، والترفيهية، لجذب الشباب للحد من الإدمان على مواقع التواصل الاجتماعي، عقد المحاضرات لتوعية بمخاطر الجرائم الإلكترونية.

ثانياً: الدراسات الأجنبية

وهدفت دراسة بوكيميجا (2018) Boukemidja التعرف على خصوصية الجرائم الإلكترونية ضد المرأة، فهل هذا النوع من الجنح يخضع لقواعد تقليدية في سياق التكيف أو يتم فرض قواعد جديدة فيما يتعلق بطبيعة الجرائم، وأثبتت نتائجها أن الجرائم ضد المرأة تتغير باستمرار، خاصة مع ظهور الوسائل الإلكترونية للكشف عنها. وبذلك أصبح العنف ضد المرأة باستخدام الوسائل الإلكترونية ظاهرة متعددة الأوجه ومظاهر وأسباب متعددة أيضا، ولا بد من قياسها من جميع جوانبها لمكافحتها بشكل فعال. بالطبع، يحدث العنف أيضًا في سياق علاقة القوة والسيطرة، وهو ما يفسر سبب هيمنة العنف الإلكتروني على العنف الأنثوي، والذي لا يزال محتجزًا إلى حد كبير. يمكن أن يكون هذا العنف نفسيًا، فهو يتألف من تشويه سمعة المرأة وإهانتها والتقليل من قيمتها الإنسانية. يتجلى في الهجوم اللفظي والشتائم والتهديدات والضغط والابتزاز والسيطرة على الأنشطة وعزل الأقارب والأصدقاء والعالم الخارجي. وكذلك الإساءة اللفظية في شكل إلكتروني، وهي التكرار المستمر لكلمات مهينة أو إهانة للمرأة. في إساءة معاملة المرأة، يؤذيها الشخص الموجود خلف الشاشة بقدر ما يؤذيها، لأن المرأة في هذه الحالة تفقد احترامها لذاتها. يمكن أن تؤدي الإساءة اللفظية إلى مجموعة من المشكلات السلوكية والعاطفية والجسدية. يؤدي العنف في هذا السياق إلى استخدام كلمات مؤذية أو مهينة، مثل تسمية الشخص السخيف أو إهانة المرأة أو الإدلاء بتعليقات عنصرية أو المضايقة المستمرة. بالإضافة إلى التحرش العام والتحرش الجنسي بشكل أكثر تحديدًا، الذين قد يتعرضون للعنف ضد المرأة، بالوسائل الإلكترونية. المشكلة تتعلق بالتوصيف القانوني لهذا النوع من العنف، ما تكفيه النصوص القديمة، ثم يتم تطبيقه تلقائيًا؛ أو هناك حاجة إلى نصوص جديدة.

وحاولت دراسة بولبنيثا وآخرون (2020) Poulpunitha, et al. الاستراتيجيات المثالية لمنع جرائم الإنترنت ضد النساء والفتيات حيث أظهرت أن عددًا قليلاً فقط من المستخدمين ليسوا على دراية بالجرائم الإلكترونية. وأن هناك عدد كبير من الأدوات والموارد المتاحة لفرز مثل هذه الأمور المثيرة للقلق. من خلال اعتماد القليل من الإجراءات الوقائية

وأفضل الممارسات، يمكننا بالتأكيد منع الجرائم الإلكترونية. لتنفيذ استراتيجيات وقائية أكثر فعالية، من الضروري أن يفهم اختصاصيو التوعية وأولياء الأمور وإنفاذ القانون والمشرعون السبب الجذري لحدوث مثل هذه الجرائم الإلكترونية. يجب على المدارس والكليات تثقيف الطلاب وأولياء الأمور بانتظام حول تصفح آمن، من خلال ورش العمل والندوات. يجب أن يكون الوعي بالجرائم الإلكترونية جزءًا من الدورات التدريبية المنتظمة في المؤسسات التعليمية، ويجب مراقبة مرافق الإنترنت المجانية المقدمة للمؤسسات التعليمية بعناية والحفاظ عليها آمنة. يجب زيادة عدد الخلايا السيبرانية والمحكمة الإلكترونية المكلفة بمعالجة مثل هذه الإجراءات. قد تساعد عمليات الربط المثمرة بين شركات تكنولوجيا المعلومات وسلطات إنفاذ القانون في تتبع ومعاقبة الأفراد الذين ينغمسون في مثل هذه الجرائم.

ومن خلال دراسة بانجلا وتيلي Bhangla, & Tuli (2021) وهي دراسة وصفية مقطعية لتجارب النساء مع الجرائم الإلكترونية في مقاطعة نيروبي، كينيا، حاولت الدراسة تحديد أشكال الجرائم الإلكترونية التي تتعرض لها النساء، ومدى انتشار الجرائم الإلكترونية ضدهن، بالإضافة إلى تأثيرات هذه الجرائم عليهن، حيث أكدت النتائج المضايقات عبر الإنترنت، والمطاردة الإلكترونية، وتلقي الشتائم، والتهديدات عبر الإنترنت، والتحرش الجنسي، وكشف الخصوصية، وانتحال الشخصية، وتخريب السمعة، ونشر الصور الخاصة على الإنترنت دون موافقتهن، وتعطيل الحاسب الآلي، والمضايقات عبر الإنترنت والمطاردة عبر الإنترنت هي الجرائم الأكثر شيوعًا ضد النساء، وأوصت الدراسة بأن النساء اللائي يستخدمن الموارد عبر الإنترنت يجب أن يستفدن من إعدادات الأمان الموضوعة للحد من التعرض عبر الإنترنت، وزيادة مخاطر الجاني .يجب على الحكومة من خلال وكالات إنفاذ القانون أن تتعقب وتنفذ قانون إساءة استخدام الكمبيوتر والجرائم الإلكترونية من أجل حماية مستخدمي الإنترنت من الجرائم الإلكترونية.

وحاولت دراسة دار وناجرث Dar & Nagrath (2022) مناقشة مدى سهولة المرأة كهدف لجرائم الإنترنت في الهند حيث تطرقت الدراسة إلى أشكال العنف الجنسي أو العنف القائم على النوع الاجتماعي ضد المرأة والذي يحدث من خلال تكنولوجيا المعلومات والاتصالات مثل الإنترنت والأجهزة المحمولة وألعاب الفيديو بالعنف السيبراني. تُعد هذه التقنيات مثالية للاستخدام كأسلحة ضد النساء لأسباب متنوعة منها المطاردة عبر الإنترنت، والاعتداء الجنسي (بما في ذلك إرسال رسائل بريد إلكتروني جنسية صريحة أو إباحية إلى الضحية)، والابتزاز عبر الإنترنت، والتسلط عبر الإنترنت، والاتجار عبر الإنترنت، والتصيد الاحتيالي، حيث أكدت أن المرأة تجد أن التعرض لجرائم الإنترنت هو أكثر شيء يزعجها على الإطلاق في الهند، وأن القواعد للنظام القانوني في الهند بها ثغرات في الجرائم الإلكترونية ضد المرأة، وأوصت الدراسة صانعي السياسات وإنفاذ القانون ردع منتهكي القانون عبر الإنترنت، حيث أن تطور القانون السيبراني يجب أن يكون جنبًا إلى جنب مع تطور الجرائم الإلكترونية، وأن يتعامل قانون الإنترنت مع هذه التهديدات عبر الإنترنت. في أسرع وقت ممكن.

تختلف هذه الدراسة عن البحوث والدراسات السابقة في تركيزها على الاستراتيجيات المقترحة لتوعية المرأة السعودية بنظام مكافحة الجرائم المعلوماتية في المجتمع من خلال ثلاث أبعاد مختلفة وهي الاستراتيجية الذاتية للمرأة والاستراتيجية المجتمعية من خلال الجمعيات الأهلية المتخصصة في مجال المرأة والمعلومات، بالإضافة إلى الاستراتيجية المؤسسية من خلال الدولة، هذا بالإضافة إلى تطرقها إلى مستوى وعي المرأة السعودية بأنواع الجرائم المعلوماتية التي يمكن أن تتعرض لها المرأة، وأنظمة مكافحة هذه الجرائم بالمملكة، وتشابهت هذه الدراسة مع بعض الدراسات السابقة في تعرضها لمجتمع الدراسة وهي المرأة بشكل عام، وبعض الدراسات السابقة الأخرى التي تعرضت للمرأة السعودية، ولكنها اختلفت في أهدافها وتساؤلاتها، وتمت الاستفادة مِن الدراسات السابقة وأُطرها النظرية كأداة

للحصول على المراجع العلمية مما يُساهم فِي بلورة مشكلة الدراسة وإطارها النظري في التعرف على مشكلة الدراسة في بعض دول العالم الأخرى كالهند وكينيا، بالإضافة التعرف على الأنواع المختلفة لجرائم المعلومات التي قد تتعرض لها المرأة السعودية، والاستفادة من التوصيات المختلفة التي خرجت بها هذه الدراسات، وتم الاستفادة من الدراسات السابقة في بناء عبارات محاور أداة الدراسة ، ومناقشة النتائج النهائية للدراسة وربطها بما توصلت إليه الدراسات السابقة التي تم عرضها.

الإجراءات المنهجية للدراسة:

نوع ومنهج الدراسة:

اتبعت الدراسة منهج المسح الاجتماعي وهو أحد أنواع البحوث الوصفية الذي يقدم معلومات وحقائق حول واقع الظاهرة الحالية، حيث يستخدم هذا المنهج لدراسة الظروف الاجتماعية التي تؤثر في مجتمع معين والتي تهدف إلى جمع البيانات الاجتماعية وتحليلها للحصول على المعلومات، إذ يحاول الكشف عن الوضع القائم لمحاولة النهوض به ووضع خطة أو برنامج للإصلاح الاجتماعي (الشلهوب، 2018: 165) وهذا ما تسعى له دراستنا الحالية من خلال التعرف على مستوى وعي المرأة السعودية بأنواع الجرائم المعلوماتية التي يمكن أن تتعرض لها، ومستوى الوعي بنظام مكافحة الجرائم المعلوماتية بالمملكة، والخروج باستراتيجيات مقترحة لتوعية المرأة بنظام مكافحة الجرائم المعلوماتية المعمول به في المجتمع السعودي.

أداة الدراسة:

تم استخدام الاستبانة كأداة للدراسة لتحقيق أهداف الدراسة والإجابة على تساؤلاتها وتكونت مِن ثلاث أجزاء: **الجزء الأول**: يشمل البيانات الأولية لعينة الدراسة. **والجزء الثاني**: يشمل أسئلة مغلقة عن استخدام الإنترنت لعينة الدراسة، **والجزء الثالث**: يشمل محاور الدراسة وهي:

المحور الأول: أهم أنواع الجرائم المعلوماتية التي يمكن أن يتم تتعرض لها المرأة بالسعودية، والذي يتكون (9) عبارات.

المحور الثاني: المعرفة بنظام مكافحة الجرائم المعلوماتية بالمملكة، والذي يتكون (8) عبارات.

المحور الثالث: استراتيجيات مقترحة لتوعية المرأة السعودية بنظام مكافحة الجرائم المعلوماتية، بإجمالي (22) عبارة موزعة على ثلاث أبعاد وهي **البعد الأول**: استراتيجية ذاتية (9) عبارات، **والبعد الثاني**: استراتيجية مجتمعية من الجمعيات الأهلية المتخصصة في مجال المرأة والمعلومات ويتكون (5) عبارات، **والبعد الثالث**: استراتيجية مؤسسية من الدولة وتتكون من (8) عبارات.

تم التأكد مِن صدق أداة الدراسة مِن خلال الصدق الظاهري (صدق المحكمين) وذلك بعرضها فِي صورتها الأولية على مجموعة مِن المحكمين مِن الأساتذة المختصين في الخدمة الاجتماعية وأمن المعلومات لإبداء الرأي فيما يتعلق بمدى مناسبة العبارات وتم إعادة الصياغة لهذه العبارات، كما تم التأكد مِن صدق الاتساق الداخلي وهو مدى اتساق كل فقرة مِن الفقرات مع المحور الذي تنتمي إليه هذه الفقرة، وذلك بحساب معاملات ارتباط بيرسون بين درجة كل فقرة والدرجة الكلية للمحور الذي تنتمي إليه، ولقياس الاتساق الداخلي للاستبانة تم استخراج معامل ارتباط بيرسون لدرجة كل عبارة مِن عبارات الاستبانة مع الدرجة الكلية للمحور التي تنتمي إليه،

وجاءت النتائج كما يلي:

جدول رقم (1)

يوضح نتائج تحليل بيرسون لحساب معاملات الارتباط لعبارات أداة الدراسة

المحور الأول		المحور الثاني		المحور الثالث			
م	الارتباط للمحور	م	الارتباط للمحور	م	الارتباط للمحور	م	الارتباط للمحور
1	**0.562	1	**0.634	1	**0.362	12	**0.629
2	**0.658	2	**0.757	2	**0.513	13	**0.629
3	**0.659	3	**0.715	3	**0.476	14	**0.534
4	**0.609	4	**0.755	4	**0.650	15	**0.528
5	**0.629	5	**0.709	5	**0.599	16	**0.655
6	**0.672	6	**0.759	6	**0.607	17	**0.667
7	**0.730	7	**0.682	7	**0.668	18	**0.686
8	**0.745	8	**0.724	8	**0.589	19	**0.659
9	**0.723	9	**0.700	9	**0.608	20	**0.515
				10	**0.617	21	**0.655
				11	**0.683	22	**0.586

من الجدول رقم (1) يتضح أن جميع معاملات الارتباط بين العبارة والمحور التي تنتمي إليه موجبة ودالة إحصائيًا عند مستوى دلالة (0.01)، وهو ما يؤكد صدق التكوين الداخلي الاتّساق للاستبانة، كما تم التأكد مِن الثبات لأداة الدراسة باستخدام معامل ألفا-كرونباخ Cronbach's Alpha، والجدول التالي يبين قيم معامل ألفا كرونباخ لمحاور أداة الدراسة.

جدول رقم (2)

يوضح معامل ألفا-كرونباخ لمحاور الاستبانة والاستبانة ككل

المحور	معامل ألفا كرونباخ	عدد العبارات
المحور الأول	0.838	9
المحور الثاني	0.853	8
المحور الثالث	0.908	22
الاستبانة ككل	0.915	30

يتضح مِن الجدول السابق أن قيمة معامل ألفا-كرونباخ لكامل الاستبانة بلغت (0.915)، وبلغت قيمة معامل ألفا-كرونباخ لعبارات المحور الأول (0.838)، وعبارات المحور الثاني (0.853) وعبارات المحور الثالث (0.908)، وهو ما يشير لوجود ثبات مرتفع لأداة الدراسة.

المعالجة الإحصائية:

لكي تتحقق أهداف الدراسة، وللكشف عن النتائج المراد الوصول إليها، فإنه تم إدخال القيم المتحصلة مِن

أداة الدراسة (الاستبانة) فِي برامج خاصة لإجراء المعَالجات الإحصائية اللازمة، وتم استخدام برنامج الحزم الإحصائية للعلوم الاجْتماعية SPSS، بالإضافة إلى استخدام الأساليب الإحصائية المختلفة لتقنين أداة الدراسة مثل معامل الارتباط لـ "بيرسون"، ومعامل "ألفا كرونباخ" (Cronbach Alpha)، فإنه تم استخدام التكرارات والنسب المئوية، لعرض البيانات الأولية لعينة الدراسة بالإضافة إلى المتوسط الحسابي، والانحرافات المعياري لعبارات محاور الدراسة.

مجتمع الدراسة وعينتها:

يتكون مجتمع الدراسة مِن النساء السعوديات فوق (18) عام والبالغ عددهم وفقاً لإحصائية هيئة الإحصاء (2021) تقريباً 6.5 مليون سيدة سعودية، واستعانة الدراسة بأسلوب العينة الصدفية من مجتمع الدراسة وبناء على معادلة ريتشارد جيجر تم حساب العينة اللازمة من مجتمع الدراسة، وتم توزيع أداة الدراسة على العينة المستهدفة وبلغ حجم العينة (449) استبانة قابلة للتحليل الإحصائي وهي حجم عينة مناسبة وفقاً لمعادلة ريتشارد جيجر.

1- الخصائص الديموغرافية لعينة الدراسة

جدول رقم (3)

يوضح الخصائص الديموغرافية لعينة الدراسة

البيان		العدد	النسبة
الفئة العمرية	من 18-30 عام	340	%75.7
	من 31 إلى 40 عام	29	%6.5
	من 41 إلى 50 عام	40	%8.9
	من 51 عام فأكثر	40	%8.9
الدرجة العلمية	ثانوي فأقل	41	%9.1
	دبلوم	16	%3.6
	مؤهل جامعي	364	%81.1
	دراسات عليا	28	%6.2
الحالة الاجتماعية	عزباء	343	%76.4
	متزوجة	88	%19.6
	مطلقة	11	%2.4
	أرملة	7	%1.6
الحالة الوظيفية	طالبة	339	%75.5
	خريجة لا أعمال	37	%8.2
	ربة منزل	1	%0.2
	قطاع حكومي	49	%10.9
	قطاع خاص	11	%2.4
	متقاعدة	12	%2.7
الإجمالي		449	100

عرض الجدول رقم (3) البيانات الديموغرافية لعينة الدراسة مِن النساء السعوديات فوق 18 عام، وجاءت النسبة الأكبر من الشابات اللاتي عمرهن من 18-30 عام بنسبة 75.7% من المشاركات، بينما بلغت نسبة

المشاركات من الفئة العمرية من 40 إلى 50 عام والفئة العمرية أكثر من 50 عام 8.9% لكل منهما، وأخيراً بلغت نسبة الفئة العمرية من 30 إلى 40 عام بنسبة 6.5%، كما تنوعت المستويات التعليمية للمشاركات في الدراسة وجاءت النسبة الأكبر من حاملي المؤهل الجامعي بنسبة 81.1%، كما جاءت نسبة المشاركات من لديهن مؤهل ثانوي فأقل بنسبة 9.1%، والمشاركات حاملي الدراسات العليا 6.2%، وأخيراً 3.6% من المشاركات لديهن مؤهل دبلوم، كما جاءت النسبة الأكبر من المشاركات من لم يتزوجن بنسبة 76.4%، بينما 19.6% متزوجات و 2.4% مطلقات و 1.6% آرامل، وانعكاس على الفئات العمرية لعينة الدراسة جاءت النسبة الأكبر من الطالبات بنسبة 75.5%، و10.9% يعملن بقطاع حكومي، و 8.2% خريجات لا يعملن، و 2.7% متقاعدات و 2.4% يعملن بقطاع خاص، وأخيراً 0.2% ربات منزل.

2- خصائص استخدام الإنترنت لعينة الدراسة

جدول رقم (4)

يوضح خصائص استخدام الإنترنت لعينة الدراسة

البيان		العدد	النسبة
مستوى المعرفة بالإنترنت والحاسب الآلي	ضعيف	4	%0.9
	مقبول	50	%11.1
	جيد	242	%53.9
	ممتازة	152	%33.9
أهم استخدامات الإنترنت	التواصل الاجتماعي	423	%94.20
	الدراسة أو العمل	383	%85.30
	الأخبار والترفيه	310	%69.0
	التسوق الإلكتروني	322	%71.70
معدل الاستخدام اليومي للإنترنت	لا استعمل إلا نادراً	5	%1.1
	أقل من ساعة يومياً	2	%0.4
	من ساعة إلى 3 ساعة يومياً	80	%17.8
	أكثر من 3 ساعات إلى 6 ساعات	198	%44.1
	أكثر من 6 ساعات يومياً	164	%36.5
هل عند معرفة بمفهوم الجرائم المعلوماتية	لا	64	%14.30
	نعم	385	%85.70
هل تعرضت أنت أو أحد أقاربك لجريمة معلوماتية من قبل	لا	297	%66.10
	نعم	152	%33.90
الإجمالي		**449**	**100**

عرض الجدول رقم (4) خصائص استخدام الإنترنت لعينة الدراسة مِن النساء السعوديات فوق 18 عام، وجاءت النسبة الأكبر المشاركات في الدراسة بمعرفة جيدة للإنترنت والحاسب الآلي بنسبة 53.9%، بينما 33.9% بنسبة بمعرفة ممتازة، و11.1% بمعرفة مقبولة، ونسبة صغيرة جداً بلغت 0.9% للآتي لديهن معرفة ضعيفة، كما أن أكثر استخدام الإنترنت لدى المشاركات للتواصل الاجتماعي بنسبة 94.2% من المشاركات، تليها الدراسة أول العمل بنسبة 85.35%، ثم التسوق الإلكتروني بنسبة 71.7%، وأخيراً الأخبار والترفيه بنسبة 69%، من المشاركات، كما أن الاستخدام لديهن كان النسبة الأكبر منهن 44.1% باستخدام أكثر من 3

ساعات إلى 6 ساعات يومية، بينما 36.5% منهن باستخدام يومي أكثر من 6 ساعات يومية، و17.8% باستخدام يومي من ساعة إلى 3 ساعات يومية، بينما نسبة صغير 1.1% لا تستعمل إلا نادراً و ، 0.4% باستخدام أقل من ساعة يومياً، وحول معرفة المشاركات بمفهوم الجرائم المعلوماتية بلغ 85.7% منهن لديهم المعرفة بهذا المفهوم، بينما 14.3% ليس لديهن معرفة بالمفهوم بالضبط، كما أن 66.1% من المشاركات لم يتعرضن أو أحد من أقاربهن لجريمة معلوماتية، والنتائج السابقة تظهر تميز المشاركات في الدراسة المعرفة بالإنترنت ومعدلات الاستخدام اليومي ومعرفتهن بالمفهوم وهو ما يفيد البحث وتساؤلاته المختلفة.

عرض ومناقشة نتائج الدراسة:

تم تحليل أداة الدراسة لاستخراج نتائجها وفقاً لأسئلة الدراسة وجاءت النتائج كالآتي:

الإجابة عن التساؤل الأول حول مستوى وعي المرأة السعودية بأنواع الجرائم المعلوماتية التي يمكن أن تتعرض لها المرأة.

جدول رقم (1)

يوضح المتوسطات الحسابية والانحراف المعياري لاستجابات عينة الدراسة حول عبارات محور وعي المرأة السعودية بأنواع الجرائم المعلوماتية التي يمكن أن تتعرض لها المرأة

العبارة	أعلم	محايد	لا أعلم	المتوسط الحسابي	الانحراف المعياري	درجة المعرفة	ترتيب العبارة
1. المطاردة الإلكترونية، وتشمل محاولة الاتصال عبر مواقع التواصل الاجتماعي دون أي غرض مشروع، ووضع رسائل تهديد على صفحة الدردشة.	327	95	27	2.67	0.58	أعلم	6
2. التشهير السيبراني، ويتم من خلال تشويه السمعة والابتزاز باستخدام الصور وتعديلها	341	76	32	2.69	0.60	أعلم	5
3. القرصنة الإلكترونية، وتتم بالنقر على عنوان رابط إلكتروني غير مصرح به أو تنزيل تطبيقات قد تستخدم في اختراق المعلومات الشخصية من خلال الجوال أو الحاسب الآلي	349	80	20	2.73	0.53	أعلم	2
4. التنمر الإلكتروني هو عمل من أعمال المضايقة من خلال الأجهزة الرقمية وذلك بنشر محتوى أو صور أو مقاطع فيديو مسيئة ومضللة	325	90	34	2.65	0.62	أعلم	7
5. الاستمالة عبر الإنترنت وهي أن يطلب منها بناء علاقة من خلال أحد المنصات الإلكترونية	242	130	77	2.37	0.76	أعلم	9
6. الرسائل البنكية الكاذبة عبر الجوال لسرقة البيانات الخاصة بالحسابات البنكية.	382	46	21	2.80	0.50	أعلم	1
7. تسجيل المكالمات والصور عبر وسائل الاتصال الرقمية دون علمها.	311	106	32	2.62	0.61	أعلم	8
8. زرع تطبيقات أو برامج للتنصت على جهازها الرقمي عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي.	354	63	32	2.72	0.59	أعلم	4
9. أخذ نسخة من الملفات سواء من الجوال أو جهاز الحاسب الآلي دون علمها أثناء الصيانة.	358	62	29	2.73	0.57	أعلم	2
مستوى وعي المرأة السعودية بأنواع الجرائم المعلوماتية التي يمكن أن تتعرض لها المرأة				**2.66**	**0.40**	**مرتفع**	

يتضح من الجدول رقم (5) أن المشاركات في الدراسة لديهن وعي مرتفع بأنواع الجرائم المعلوماتية التي يمكن أن تتعرضن لهن أو أي مرأة سعودية بمتوسط حسابي بلغ (2.66 من 3) وهو متوسط حسابي يقع في الفئة الثالثة وفقاً لمقياس ليكرت الثلاثي الذي يشير إلى درجة أعلم "مرتفع"، حيث تم تناول هذه الوعي من خلال تسع عبارات مختلفة تتناول أنواع الجرائم المعلوماتية المختلفة جاءت جميعها بمتوسطات حسابية تشير إلى درجة أعلم "مرتفع" فجاءت المتوسطات الحسابية لهذه العبارات ما بين (2.37 إلى 2.8 من 3)، وهو ما أثر على المتوسط الحسابي الكلي للمحور وجاء بدرجة مرتفعة.

وجاءت العبارة "6. الرسائل البنكية الكاذبة عبر الجوال لسرقة البيانات الخاصة بالحسابات البنكية." في الترتيب الأول بين عبارات المحور بمتوسط حسابي بلغ (2.8) تليها العبارتان "3. القرصنة الإلكترونية، وتتم بالنقر على عنوان رابط إلكتروني غير مصرح به أو تنزيل تطبيقات قد تستخدم في اختراق المعلومات الشخصية من خلال الجوال أو الحاسب الآلي" و "9. أخذ نسخة من الملفات سواء من الجوال أو جهاز الحاسب الآلي دون علمها أثناء الصيانة" بمتوسط حسابي بلغ (2.73) لكل منهما، وفي الترتيب الرابع جاءت العبارة "8. زرع تطبيقات أو برامج للتنصت على جهازها الرقمي عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي." بمتوسط حسابي بلغ (2.72) وتنوعت باقي عبارات هذا المحور التي أشارت إلى درجة أعلم "مرتفعة" حيث جاءت العبارة "5. الاستمالة عبر الإنترنت وهي أن يطلب منها بناء علاقة من خلال أحد المنصات الإلكترونية" في الترتيب الأخير بين عبارات المحور بمتوسط حسابي بلغ (2.37).

كما تنوعت قيم الانحراف المعياري للعبارات فجاءت القيم ما بين (0.5 و0.76) لتدل الاتفاق في الآراء للمشاركات حول بعض العبارات والاختلاف في الآراء في بعض العبارات الأخرى حيث يدل ارتفاع قيمة الانحراف المعياري على الاختلاف في اتجاه الاستجابات للمشاركات، بينما الانخفاض إلى تقارب الآراء حول العبارة.

ومما سبق يتضح أن المرأة السعودية لديها وعي بأنواع الجرائم المعلوماتية التي يمكن أن تتعرض لها، كالرسائل البنكية الكاذبة عبر الجوال لسرقة البيانات الخاصة بالحسابات البنكية، القرصنة الإلكترونية، واختراق المعلومات الشخصية من خلال الجوال أو الحاسب الآلي، هذا بالإضافة إلى نسخ الملفات الخاصة من الجوال أو الحاسب الآلي دون علمها أثناء الصيانة، وزرع تطبيقات أو برامج للتنصت على جهازها الرقمي، وجرائم تشويه السمعة والابتزاز باستخدام الصور وتعديلها، المطاردة الإلكترونية، والتنمر الإلكتروني ونشر محتوى أو صور أو مقاطع فيديو مسيئة ومضللة، وكذلك تسجيل المكالمات والصور عبر وسائل الاتصال الرقمية دون علمها، والاستمالة عبر الإنترنت وهي أن يطلب منها بناء علاقة من خلال أحد المنصات الإلكترونية، وهي جميعها جرائم قد تقع فيها المرأة السعودية، وأكدت النتائج وعيها بهذه الجرائم وما ما تناولت أيضاً نتائج بعض الدراسات السابقة كدراسة عبد الرازق (2017) التي تناول هذه الجرائم الإلكترونية ضد النساء والفتيات حيث رصدتها بمسميات مختلفة، كما تناولته أيضا دراسة الجاسر (2021) التي أكدت نتائج أن جرائم الاختراق السيبراني تصدرت قائمة أنماط الجرائم السيبرانية الممارسة ضد المرأة السعودية عبر وسائل الإعلام الجديد، واتخذت الجرائم الجنسية المرتبة الثانية، تلا ذلك الجرائم المالية، ثم جرائم تشويه السمعة، وجاءت سرقة المعلومات الشخصية في المرتبة الأخيرة، وهو ما تناولته أيضاً دراسة بوكيميجا Boukemidja (2018)، ودراسة بانجلا وتيلي Bhangla, & Tuli (2021).

ودراسة دار وناجرث .Dar& Nagrath. (2022)، في حين توافقت نتائج الدراسة الحالية حول مستوي الوعي مع ما جاءت به دراسة الزبن (2021) مستوى الوعي بالجرائم الإلكترونية المرتفع لدى المشاركين بالدراسة، فقد جاء مرتفع. الإجابة عن التساؤل الثاني حول مستوى وعي المرأة السعودية بنظام مكافحة الجرائم المعلوماتية.

جدول رقم (2)

يوضح المتوسطات الحسابية والانحراف المعياري لاستجابات عينة الدراسة حول عبارات محور وعي المرأة السعودية بنظام مكافحة الجرائم المعلوماتية

العبارة	أعلم	محايد	لا أعلم	المتوسط الحسابي	الانحراف المعياري	درجة المعرفة	ترتيب العبارة
1. التنصت على الأشخاص عبر الإنترنت دون مسوغ نظامي	301	64	84	2.48	0.79	أعلم	7
2. تهديد الأشخاص أو ابتزازهم أو إجبارهم على القيام بأعمال مشينه	393	29	27	2.82	0.52	أعلم	1
3. التعدي على لحياة الخاصة عن طريق إساءة استخدام كاميرا الهواتف النقالة أو غيرها	377	43	29	2.78	0.55	أعلم	3
4. التشهير عبر الوسائل الرقمية.	382	42	25	2.80	0.52	أعلم	2
5. الدخول على الحسابات البنكية الشخصية دون أذن منهم.	376	36	37	2.76	0.59	أعلم	4
6. الدخول غير المشروع لإلغاء بيانات خاصة، أو تسريبها أو إعادة نشرها.	359	49	41	2.71	0.62	أعلم	5
7. يعاقب كل من شرع في القيام بالجرائم الرقمية بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة.	296	62	91	2.46	0.81	أعلم	8
8. يعاقب القانون كل من حرَّض غيره، أو ساعده، أو اتفق معه على ارتكاب أيٍّ من الجرائم الرقمية.	364	39	46	2.71	0.64	أعلم	5
مستوى وعي المرأة السعودية بنظام مكافحة الجرائم المعلوماتية				**2.69**	**0.45**	**مرتفع**	

يتضح من الجدول السابق أن المشاركات في الدراسة لديهن وعي مرتفع بنظام مكافحة الجرائم المعلوماتية بمتوسط حسابي بلغ (2.69 من 3) وهو متوسط حسابي يقع في الفئة الثالثة وفقاً لمقياس ليكرت الثلاثي الذي يشير إلى درجة أعلم "مرتفع"، حيث تم تناول هذه الوعي من خلال ثمان عبارات مختلفة تتناول الإجراءات أو الجزاءات المختلفة التي ينص عليها نظام مكافحة الجرائم المعلوماتية بالمملكة العربية السعودية جاءت جميعها بمتوسطات حسابية تشير إلى درجة أعلم "مرتفع" فجاءت المتوسطات الحسابية لهذه العبارات ما بين (2.46 إلى 2.82 من 3)، وهو ما أثر على المتوسط الحسابي الكلي للمحور وجاء بدرجة مرتفعة.

وجاءت العبارة "2. تهديد الأشخاص أو ابتزازهم أو إجبارهم على القيام بأعمال مشينه" في الترتيب الأول بين عبارات المحور بمتوسط حسابي بلغ (2.82) تليها العبارة "4. التشهير عبر الوسائل الرقمية." بمتوسط حسابي بلغ (2.8) وفي الترتيب الثالث جاءت العبارة "3. التعدي على لحياة الخاصة عن طريق إساءة استخدام كاميرا الهواتف النقالة أو غيرها " بمتوسط حساب بلغ (2.78)، وتنوعت باقي عبارات هذا المحور التي أشارت إلى درجة أعلم "مرتفعة" حيث جاءت العبارة "7. يعاقب كل من شرع في القيام بالجرائم الرقمية بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة." في الترتيب الأخير بين عبارات المحور بمتوسط حسابي بلغ (2.46).

كما تنوعت قيم الانحراف المعياري للعبارات فجاءت القيم ما بين (0.52 و0.81) لتدل الاتفاق في الآراء للمشاركات حول بعض العبارات والاختلاف في الآراء في بعض العبارات الأخرى حيث يدل ارتفاع قيمة الانحراف المعياري على الاختلاف في اتجاه الاستجابات للمشاركات، بينما الانخفاض إلى تقارب الآراء حول العبارة.

ومما سبق يتضح أن المرأة السعودية لديها وعي مرتفع بنظام مكافحة الجرائم المعلوماتية من خلال وعيها بوجود جزاءات لأنماط الجرائم المختلفة حيث أكدت أن جميع الجرائم والأفعال التي تتسم بالجرم باستخدام المعلومات والتكنولوجيا هي جرائم يعاقب عليها القانون سواء بالحبس أو الغرامة المالية أو الإثنين معاً كحالات التهديد للأشخاص أو ابتزازهم أو إجبارهم على القيام بأعمال مشينه، والتشهير عبر الوسائل الرقمية، لتعدي على لحياة الخاصة عن طريق إساءة استخدام كاميرا الهواتف النقالة أو غيره، دخول على الحسابات البنكية الشخصية دون أذن منهم، أو الدخول لإلغاء بيانات خاصة، أو تسريبها أو إعادة نشرها.، وهذا ليس فقط بل نص النظام على معاقبة المحرض بذات العقوبة، فضلاً عن أنه هناك عقاب على هذه الجرائم حتى لو لم تكتمل بما يعد الشروع في الجريمة ذاتها، وقد توافقت هذه النتائج مع بعض الدراسات السابقة التي تناولت البعد القانوني والجزائي لجرائم المعلومات كدراسة غريب، والأمير (2017) التي أكدت وعي الفئة العمرية الشابة بنظام عقوبات الجرائم المعلوماتية السعودي، ودراسة بوكيميجا Boukemidja (2018). التي تعرضت للتوصيف القانوني لهذا النوع من الجرائم، كما توافقات مع توصيات دراسة بولبنيثا وآخرون Poulpunitha, et al. (2020). التي أكدت أهمية إنفاذ القانون على هذه الجرائم ومعاقبة الأفراد الذين ينغمسون في مثل هذه الجرائم، وهو ما أوصت به أيضاً دراسة بانجلا وتيلي Bhangla, & Tuli (2021).

الإجابة عن التساؤل الثالث حول الاستراتيجيات المقترحة لتوعية المرأة بنظام مكافحة الجرائم المعلوماتية.

جدول رقم (3)

المتوسطات الحسابية والانحراف المعياري لاستجابات عينة الدراسة حول عبارات محور الاستراتيجيات المقترحة لتوعية المرأة بنظام مكافحة الجرائم المعلوماتية

العبارة	موافق	محايد	غير موافق	المتوسط الحسابي	الانحراف المعياري	درجة الموافقة	ترتيب العبارة
1. عدم الكشف عن أي معلومات شخصية عبر الإنترنت خصوصاً في مواقع التواصل الاجتماعي	402	37	10	2.87	0.39	موافق	6
2.الامتناع عن إرسال الصور الشخصية عبر الإنترنت إلى الأصدقاء أثناء الدردشة.	314	104	31	2.63	0.61	موافق	9
3. الحفاظ على سرية تفاصيل بطاقة الائتمان والحسابات البنكية وعدم إرسالها عبر مواقع التواصل الاجتماعي	395	51	3	2.87	0.35	موافق	6
4. التأكد من مصداقية مواقع الشراء الإلكتروني التي تستخدم فيها بطاقات الائتمان	418	27	4	2.92	0.30	موافق	1
5. الإبلاغ الفوري عن أي رسائل تهديد أو طلب أرقام حسابات بنكية من خلال الجوال	416	30	3	2.92	0.30	موافق	2
6. عدم فتح الروابط الإلكترونية المرسلة عبر رسائل الجوال أو مواقع التواصل الاجتماعي أو البريد الإلكتروني خصوصاً من الأشخاص غير المعروفين.	409	37	3	2.90	0.32	موافق	4
7. عدم الدخول على المواقع المشبوهة والتي قد تكون مصيدة لمرتكبي الجرائم المعلوماتية	416	25	8	2.91	0.34	موافق	3
8. العمل دائماً على صيانة الأجهزة الرقمية في أماكن صيانة معتمدة وذات ثقة	392	49	8	2.86	0.40	موافق	8
9. عدم ترك صور شخصية على الأجهزة الرقمية عند بيعها والتأكد من حذفها تماماً أو تدميرها	408	32	9	2.89	0.37	موافق	5
استراتيجية ذاتية				**2.86**	**0.25**	**موافقة**	
10. توفير دورات تدريبية لزيادة الوعي الرقمي والأمن السيبراني لدى المرأة السعودية	403	44	2	2.89	0.32	موافق	1
11. الاستفادة من الفعاليات المختلفة بالمرأة لتثقيفها بشأن الجرائم والتهديدات الإلكترونية	400	46	3	2.88	0.34	موافق	2
12 عقد فعاليات في مناطق التجمعات (كالمراكز التجارية) للتوعية بأنواع الجرائم المعلوماتية	376	61	12	2.81	0.45	موافق	5
13. إصدار تطبيقات أو صفحات التواصل الاجتماعي للتوعية بالجرائم الرقمية	393	53	3	2.87	0.36	موافق	3

جدول رقم (4)

المتوسطات الحسابية والانحراف المعياري لاستجابات عينة الدراسة حول عبارات محور الاستراتيجيات المقترحة لتوعية المرأة بنظام مكافحة الجرائم المعلوماتية

العبارة	موافق	محايد	غير موافق	المتوسط الحسابي	الانحراف المعياري	درجة الموافقة	ترتيب العبارة
14. بناء حلقة وصل بين ضحايا الجرائم الرقمية وبين الجهات المسئولة في الدولة	391	53	5	2.86	0.38	موافق	4
استراتيجية مجتمعية من الجمعيات الأهلية المتخصصة في مجال المرأة والمعلومات				**2.86**	**0.28**	**موافقة**	
15. التوعية بالقوانين والعقوبات الرادعة لمرتكبي الجرائم المعلوماتية من خلال وسائل التواصل الاجتماعي	426	22	1	2.95	0.23	موافق	1
16. تطوير المناهج التعليمية في المراحل المختلفة بإدخال موضوعات خاصة بالأمن السيبراني والجرائم المعلوماتية	389	52	8	2.85	0.41	موافق	7
17. توفير رخصة الأمان السيبراني للأشخاص القائمين بصيانة الأجهزة الرقمية.	397	43	9	2.86	0.40	موافق	6
18. توفير نشرة دورية بأهم رسائل الاحتيال المرسلة عبر الجوال والبريد الإلكتروني للتوعية	404	44	1	2.90	0.31	موافق	4
19. استحداث تطبيق للإبلاغ عن رسائل الاحتيال عبر الجوال وعبر البريد الإلكتروني لسهولة وسرعة الاستخدام	403	40	6	2.88	0.36	موافق	5
20. توفير تطبيقات لحماية الأجهزة الرقمية مجانية أو بسعر رمزي لاستخدامها عبر موزعي الإنترنت.	388	49	12	2.84	0.44	موافق	8
21. قيام البنوك داخل المملكة بزيادة التوعية حول رسائل الاحتيال البنكية المنتشرة والطرق الموثوقة لتحديث البيانات.	411	33	5	2.90	0.33	موافق	3
22. توفير خط ساخن للإبلاغ عند التعرض للجرائم الرقمية مع حماية الخصوصية.	417	31	1	2.93	0.27	موافق	2
استراتيجية مؤسسية من الدولة				**2.89**	**0.24**	**موافقة**	
الاستراتيجيات المقترحة لتوعية المرأة بنظام مكافحة الجرائم المعلوماتية				**2.87**	**0.22**	**موافق**	

يتضح من الجدول رقم (7) أن المشاركات في الدراسة أيدن الاستراتيجيات المقترحة لتوعية المرأة لمكافحة الجرائم المعلوماتية بمتوسط حسابي بلغ (2.87 من 3) وهو متوسط حسابي يقع في الفئة الثالثة وفقاً لمقياس ليكرت الثلاثي الذي يشير إلى درجة موافق، حيث تم الموافقة على أبعاد الاستراتيجيات الثلاث فجاءت الموافقة على الاستراتيجية المؤسسية من الدولة في الترتيب الأول بمتوسط حسابي بلغ (2.89) تليها الاستراتيجية المجتمعية من الجمعيات الأهلية المتخصصة في مجال المرأة والمعلومات، والاستراتيجية الذاتية، بمتوسط حسابي بلغ (2.86) لكل منهما، حيث تم تأييد هذه الاستراتيجيات بعبارات متنوعة جاءت جميعها بمتوسطات حسابية تشير إلى درجة موافقة.

فجاءت العبارتان "4. التأكد من مصداقية مواقع الشراء الإلكتروني التي تستخدم فيها بطاقات الائتمان" و"5. الإبلاغ الفوري عن أي رسائل تهديد أو طلب أرقام حسابات بنكية من خلال الجوال" في الترتيب الأول بالنسبة للاستراتيجية الذاتية بمتوسط حسابي بلغ (2.92) لكل منهما، وتنوعت عبارات هذا البعد فجاءت العبارة "2. الامتناع

عن إرسال الصور الشخصية عبر الإنترنت إلى الأصدقاء أثناء الدردشة." بأقل قيمة متوسط حسابي في هذا البعد ولكنه يشير أيضاً إلى درجة موافقة حيث بلغ قيمته (2.63)، بينما جاءت العبارة "10. توفير دورات تدريبية لزيادة الوعي الرقمي والأمن السيبراني لدى المرأة السعودية" في الترتيب الأول ببعد الاستراتيجية المجتمعية من الجمعيات الأهلية المتخصصة في مجال المرأة والمعلومات بمتوسط حسابي بلغ (2.89) تليها العبارة "11. الاستفادة من الفعاليات المختلفة بالمرأة لتثقيفها بشأن الجرائم والتهديدات الإلكترونية" بمتوسط حسابي بلغ (2.88) بينما العبارة "12 عقد فعاليات في مناطق التجمعات (كالمراكز التجارية) للتوعية بأنواع الجرائم المعلوماتية" جاءت بأقل قيمة في المتوسط الحسابي بهذا البعد بمتوسط حسابي بلغ (2.81)، وأخيراً جاءت العبارة "15. التوعية بالقوانين والعقوبات الرادعة لمرتكبي الجرائم المعلوماتية من خلال وسائل التواصل الاجتماعي" في الترتيب الأول ضمن الاستراتيجية المؤسسية من الدولة بمتوسط حسابي بلغ (2.95) تليها العبارة "22. توفير خط ساخن للإبلاغ عند التعرض للجرائم الرقمية مع حماية الخصوصية. "بمتوسط حسابي بلغ (2.93) وتنوعت قيم المتوسطات الحسابية لباقي العبارات، فجاءت العبارة "20. توفير تطبيقات لحماية الأجهزة الرقمية مجانية أو بسعر رمزي لاستخدامها عبر موزعي الإنترنت." أقل عبارة في قيم المتوسطات الحسابية بهذا البعد بمتوسط حسابي بلغ (2.84).

كما يلاحظ أن قيم الانحراف المعياري لعبارات هذا المحور منخفضة للتأكيد على اتفاق وتأييد المشاركات في العبارات باتجاه موافقة على عبارات الاستراتيجيات المقترحة بنسبة كبيرة، فجاءت القيم ما بين (023 و0.61).

ومما سبق يمكن استخلاص توافق الآراء حول الاستراتيجيات الثلاثة لتوعية المرأة لمكافحة الجرائم المعلوماتية والتي يمكن الخروج بها كتوصيات يمكن أن تسهم في توعية المرأة السعودية لمكافحة الجرائم وهذه الاستراتيجيات المختلفة توافقت مع ما أوصت به معظم الدراسات السابقة كدراسة غريب، والأمير (2017) التي بضرورة تصميم وتنفيذ برامج وقائية للشباب للتوعية بعواقب الجرائم المعلوماتية وإقامة الندوات والمؤتمرات العلمية في مجال وقاية الشباب من مخاطر الجرائم المعلوماتية، وهو ما أكدته دراسة الهيف، العنزي (2018) مضيفة أهمية الوعي الديني والأخلاقي الذي يعد من أهم العناصر التي تساعد في عدم الوقوع في الجرائم المعلوماتية، وتوافقت أيضاً هذه الاستراتيجيات مع دراسة الزبن (2021) التي أوصت بتوعية الطلبة بأهمية استثمار وقتهم عند استخدام الإنترنت لتطوير مهاراتهم، تفعيل النشاطات الرياضية، والثقافية، والترفيهية، لجذب الشباب للحد من الإدمان على مواقع التواصل الاجتماعي، عقد المحاضرات للتوعية بمخاطر الجرائم الإلكترونية، في حين دراسة بانجلا وتيلي .Bhangla, & Tuli (2021) وجهت توصياتها إلى الحكومة لإنفاذ القانون أن تتعقب وتنفذ قانون إساءة استخدام الكمبيوتر والجرائم الإلكترونية من أجل حماية مستخدمي الإنترنت من الجرائم الإلكترونية، وهو ما نادت به أيضاً دراسة دار وناجرث Dar& Nagrath. (2022).

توصيات الدراسة:

بناء على التأييد التام للمشاركات في الدراسة لعناصر الاستراتيجيات المختلفة فتوصي الدراسة بتطبيق هذه الاستراتيجيات وفقاً لمحاورها الثلاث وهي كالآتي:

توصيات خاصة بالمرأة السعودية ذاتها:

- يجب أن تتأكد من مصداقية مواقع الشراء الإلكتروني التي تستخدم فيها بطاقات الائتمان.
- يجب ألا تخجل وتبلغ فوراً عن أي رسائل تهديد أو طلب أرقام حسابات بنكية من خلال الجوال
- أن تتجنب الدخول على المواقع المشبوهة والتي قد تكون مصيدة لمرتكبي الجرائم المعلوماتية
- أن تتجنب فتح الروابط الإلكترونية المرسلة عبر رسائل الجوال أو مواقع التواصل الاجتماعي أو البريد الإلكتروني خصوصاً من الأشخاص غير المعروفين .

- عدم ترك صور شخصية على الأجهزة الرقمية عند بيعها والتأكد من حذفها تماماً أو تدميرها
- التأكيد على عدم الكشف عن أي معلومات شخصية عبر الإنترنت خصوصاً في مواقع التواصل الاجتماعي
- تجنب إرسال تفاصيل بطاقة الائتمان والحسابات البنكية عبر مواقع التواصل الاجتماعي
- أن تكون صيانة الأجهزة الرقمية في أماكن صيانة معتمدة وذات ثقة
- تجنب إرسال الصور الشخصية عبر الإنترنت إلى الأصدقاء أثناء الدردشة إلا للضرورة.

توصيات خاصة بالجمعيات الأهلية المتخصصة في مجال المرأة والمعلومات:

- أن تعمل الجمعيات على توفير دورات تدريبية لزيادة الوعي الرقمي والأمن السيبراني لدى المرأة السعودية.
- أهمية زيادة الجرعات التوعوية للمرأة السعودية من خلال الاستفادة من الفعاليات المختلفة بالمرأة لتثقيفها بشأن الجرائم والتهديدات الإلكترونية
- العمل على إصدار تطبيقات أو صفحات التواصل الاجتماعي للتوعية بالجرائم الرقمية
- أن تعمل هذه الجمعيات على حماية المرأة التي تتعرض لهذه النوعيات من الجرائم من خلال بناء حلقة وصل بين ضحايا الجرائم الرقمية وبين الجهات المسئولة في الدولة
- زيادة فعاليات التوعية في مناطق التجمعات (كالمراكز التجارية) للتوعية بأنواع الجرائم المعلوماتية.

توصيات لمؤسسات الدولة الرسمية:

- العمل على زيادة التوعية بالقوانين والعقوبات الرادعة لمرتكبي الجرائم المعلوماتية من خلال وسائل التواصل الاجتماعي.
- العمل على الإعلان الجيد لخطوط الإبلاغ عند التعرض للجرائم الرقمية مع حماية الخصوصية.
- أن تعمل البنوك السعودية بزيادة التوعية حول رسائل الاحتيال البنكية المنتشرة والطرق الموثوقة لتحديث البيانات.
- أن تعمل وزارة الاتصالات بتوفير نشرة دورية بأهم رسائل الاحتيال المرسلة عبر الجوال والبريد الإلكتروني للتوعية
- أن تنشئ وزارة الاتصالات ووزارة الداخلية تطبيق للإبلاغ عن رسائل الاحتيال عبر الجوال وعبر البريد الإلكتروني لسهولة وسرعة الاستخدام
- أن تقوم وزارة الاتصالات بتوفير رخصة الأمان السيبراني للأشخاص القائمين بصيانة الأجهزة الرقمية.
- أن تقوم وزارة التعليم بتطوير المناهج التعليمية في المراحل المختلفة بإدخال موضوعات خاصة بالأمن السيبراني والجرائم المعلوماتية
- أن تقوم وزارة الاتصالات بتوفير تطبيقات لحماية الأجهزة الرقمية مجانية أو بسعر رمزي لاستخدامها عبر موزعي الإنترنت.

مراجع الدراسة:

أنيس، إبراهيم واخرون (2004) المعجم الوسيط، ط4، مجمع اللغة العربية، مكتبة الشروق الدولية.

البدانية، ذياب موسى (2014). الجرائم الإلكترونية: المفهوم والأسباب. الجرائم المستحدثة في ظل التغيرات والتحولات الإقليمية والدولية 2014/9/4. كلية العلوم الاستراتيجية عمان، الأردن.

تجيني، أمين (2020) الجرائم المعلوماتية، مجلة استشراف للدراسات والأبحاث القانونية، (6)، 115-137.

الجاسر، شعاع (2021) الجرائم السيبرانية الممارسة ضد المرأة السعودية وعلاقتها بالسمات الشخصية للضحية المستخدمة لوسائل الإعلام الجديد، مجلة جامعة الشارقة للعلوم الإنسانية والاجتماعية، 18(1)، 195-233.

الحميدي، هشام (2011) دور هيئة الامر بالمعروف والنهي عن المنكر في الحد من جرائم الابتزاز ضد الفتيات في المملكة العربية السعودية، رسالة ماجستير غير منشوره، جامعة نايف العربية للعلوم الأمنية، الرياض.

الخالدي، عبير (2020) دور الوعي الاجتماعي في مواجهة الابتزاز الالكتروني، المجلة العلمية لكلية التربية، جامعة بغداد، بغداد.

الدعجة، أمجد حسن مرشد (2014) استراتيجية مكافحة الجرائم المعلوماتية، رسالة ماجستير غير منشورة، جامعة أم درمان الإسلامية.

زايد، أحمد. (2017). جرائم الكمبيوتر والإنترنت في المجتمع المصري: دراسة لأبعادها النفسية والاجتماعية والقانونية. (سميحة نصر، المحرر) القاهرة: المركز القومي للبحوث الاجتماعية والجنائية، قسم بحوث الجريمة.

الزبن، غدير برنس عضوب (2021) الجرائم الإلكترونية ومستوى الوعي بخطورتها: دراسة ميدانية على عينة من الشباب الجامعي الأردني، مجلة الجامعة الإسلامية للبحوث الإنسانية، 2(29)، 230-248.

السروجي، طلعت مصطفى (2004) السياسة الاجتماعية في إطار المتغيرات العالمية الجديدة، الطبعة الأولى، دار الفكر العربي، القاهرة.

سليمان، مروة (2022). نظرية الأنشطة الروتينية: نظرية جديدة لفهم الجرائم السيبرانية. المجلة المصرية للعلوم الاجتماعية والسلوقية, 6(6), 114-130.

الشلهوب، هيفاء (2018) "طرق البحث في الخدمة الاجتماعية" مكتبة الشقري، الرياض.

شمروخ، مرفت جمال الدين على (2017) رؤية استراتيجية لدور منظمات المجتمع المدني وتعزيز الأمن الفكري للشباب، مجلة الخدمة الاجتماعية، الجمعية المصرية للأخصائيين الاجتماعيين 56(3)، 435-479.

عبد اللطيف، سهير صفوت عبد المجيد؛ عبد الله، سحر حساني بربري (2019) الجرائم الإلكترونية المرتكبة ضد المرأة عبر الإنترنت: دراسة حالة لعينة من النساء مستخدمات الإنترنت في مصر، مجلة كلية الآداب، جامعة الإسكندرية، (95)، 1-39.

عجوة، علي (2014) الأعلام الأمني "المشكلات والحلول" الأكاديميون للنشر والتوزيع، عمان.

غريب، ماجدة عزت؛ والأمير، حسن (2017) مدى الوعي لدى الفئة العمرية الشابة بنظام عقوبات الجرائم المعلوماتية السعودي، المجلة العربية الدولية للمعلوماتية، 5(9)، 17-33.

غزال، عبد الرزاق (2017) الجرائم الإلكترونية ضد النساء والفتيات: المخاطر وطرق المواجهة، مؤتمر المرأة والإعلام وتحديات ثورة الاتصال.

فكري، أيمن عبد الله (2014) الجرائم المعلوماتية: دراسة مقارنة في التشريعات العربية والأجنبية، الرياض: مكتبة القانون والاقتصاد.

الهيف، عالية بنت مذكر هيف (2022) الجرائم المعلوماتية أنواعها وخطورتها: دراسة لقياس مستوى وعي طلبات قسم المكتبات والمعلومات في جامعة الأميرة نورة بنت عبد الرحمن 1438هـ -1439/ 2017 – 2018، المجلة الأردنية للمكتبات والمعلومات، جمعية المكتبات والمعلومات الأردنية، 53(3)، 45-91.

هيئة الخبراء بمجلس الوزراء (2022) نظام مكافحة جرائم المعلوماتية، مجموعة الأنظمة السعودية، مج7، أنظمة المواصلات والاتصالات نظام مكافحة جرائم المعلوماتية، رابط: https://laws.boe.gov.sa/BoeLaws/Laws

Donner, C. M., Marcum, C. D., Jennings, W. G., Higgins, G. E., & Banfield, J. (2014). Low self-control and cybercrime: Exploring the utility of the general theory of crime beyond digital piracy. *Computers in Human Behavior*, *34*, 165-172.

Reep-van den Bergh, C. M., & Junger, M. (2018). Victims of cybercrime in Europe: a review of victim surveys. *Crime science*, *7*(1), 1-15.

Halder, D., & Karuppannan, J. (2009). Cyber socializing and victimization of women. *The Journal on Victimization*, *12*(3), 5-26.

West, J. (2014). *Cyber-violence against women*. Battered Women's Support Services.

Boukemidja, N. B. (2018). Cyber Crimes against Women: Qualification and Means. *European Journal of Social Sciences*, *1*(3), 34-44.

Poulpunitha, S., Manimekalai, K., & Veeramani, P. (2020). Strategies to prevent and control of cybercrime against women and girls. *Mental*, *81*, 81-0.

Bhangla, A., & Tuli, J. (2021). A Study on Cyber Crime and its Legal Framework in India. *Issue 2 Int'l JL Mgmt. & Human.*, *4*, 493.

Dar, S. A., & Nagrath, D. (2022). Are Women a Soft Target for Cyber Crime in India. *Journal of Information Technology and Computing*, *3*(1), 23-31.

Kaushik, N. (2014). Cyber Crimes against Women. Global Journal of Research in Management, 4(1), 37-46.

Boskovic, M., & Misev, G. (2022). Secondary Victimization of Sexually Assaulted Women. In *Victimology* (pp. 341-361). Springer, Cham.

Bhat, R. M., & Ahmad, P. A. (2022). Social Media and the Cyber Crimes against Women-A Study. *Journal of Image Processing and Intelligent Remote Sensing (JIPIRS) ISSN 2815-0953*, *2*(01), 18-22.