الوعي بالجريمة السيبرانية القائمة على منصات التواصل الاجتماعي: دراسة استكشافية على المجتمع العماني

شيرين عبد الجواد أحمد & محمد بن خميس عبد الله الحربي & د. محمود علي موسى

http://dx.doi.org/10.29009/ijres.7.3.1

الوعي بالجريمة السيبرانية القائمة على منصات التواصل الاجتماعي: دراسة استكشافية على المجتمع العماني

شيرين عبد الجواد أحمد
باحثة بكلية التربية جامعة قناة السويس، مصر
sismail@du.edu.om
محمد بن خميس عبد الله الحربي
مدير مدرسة الأمل للصم، سلطنة عمان
Moh002@moe.om
د. محمود علي موسى
أستاذ علم النفس التعليمي، بكلية التربية جامعة قناة السويس، مصر
Mahmoud_muhanna@edu.suez.edu.eg

قدمت للنشر في 1/ 3/ 2024 **قبلت للنشر في 1/ 5/ 2024**

ملخص: هدفت الدراسة للتحقق من مصداقية الوعي بالجريمة السيبرانية القائمة على منصات التواصل الاجتماعي على عينة من المجتمع العماني، وتم استخدام المنهج التحليلي الاستكشافي في هذه الدراسة، وتكونت عينة الدراسة من 170 فرداً من المجتمع العماني، وقد اختيرت العينة بطريقة كرة الثلج، وقد توصلت الدراسة في ضوء الدراسات السابقة وفي ضوء تحليل المحتوى لدراسات الجريمة السيبرانية عن بعض العبارات التي تشير للوعي بالجريمة السيبرانية القائمة على منصات التواصل الاجتماعي وبلغ عددهم 16 عبارة، وقد تم استخدام التحليل العاملي الاستكشافي والتوكيدي للتحقق من مدى مناسبة المقياس لطبيعة العينة، وقد اتضح من المقياس بعدين بلغ 53.1٪ من التباين الكلي للظاهرة، وقد حقق المقياس ثباتًا مناسباً في ضوء معامل ألفا كرونباخ ومعامل أوميجا، وقد اختيرت عينة من المواطنين من مجتمع الدراسة للتحقق من تأثير المتغيرات الديموغرافية على أبعاد الوعي بالجريمة السيبرانية وقد أثبتت النتائج عدم تأثير

http://dx.doi.org/10.29009/ijres.7.3.1

المتغيرات الديموغرافية على الوعي بالجريمة السيبرانية القائمة على منصات التواصل الاجتماعي، ويمكن استنتاج أن الوعي بالجريمة السيبرانية هو نوع من الوعي السيبراني.

الكلمات المفتاحية: الجريمة السيبرانية؛ الوعي السيبراني؛ منصات التواصل الاجتماعي.

http://dx.doi.org/10.29009/ijres.7.3.1

Exploratory Study on Awareness of Social Networking-Based Cybercrime in the Omani Community

Shereen abdelgawad ahmed
Educational Researcher of Education– Suez Canal University – EGYPT
sismail@du.edu.om

Mohammed Khamis ALharbi
Director of Deaf Al-Amal School, Oman
Moh002@moe.om

Dr Mahmoud Ali Moussa
Professor of Educational Psychology, College of Education, Suez Canal University, EGYPT
Mahmoud_muhanna@edu.suez.edu.eg

Received on March 1st, 2024, Accepted on May 1st, 2024.

Abstract: The study aimed to verify the credibility of awareness of social media-based cybercrime in a sample of Omani society. This study used the exploratory analytical method. The sample consisted of 170 individuals from the Omani community, and the sample was selected through a snowball sampling method. The study tool, based on previous research and content analysis of cybercrime studies, identified 16 items indicating awareness of social media-based cybercrime. Exploratory and confirmatory factor analyses were used to assess the appropriateness of the scale for the sample, and the scale yielded two dimensions that accounted for 53.1% of the total variance of the phenomenon. The scale demonstrated adequate reliability based on Cronbach's alpha and omega coefficients. A subsample of Omani citizens was selected from the study sample to examine the impact of demographic variables on cybercrime awareness subscales. The results indicated that demographic

http://dx.doi.org/10.29009/ijres.7.3.1

variables did not affect social networking-based cybercrime awareness. It can be concluded that awareness of cybercrime is a form of cyber awareness.

Keywords: Cyber Crime; Cyber Awareness; Social Networking-Based.

http://dx.doi.org/10.29009/ijres.7.3.1

المقدمة

تمر المجتمعات في هذا العصر الرقمي بعدة مصطلحات جديدة منها المواطنة الرقمية، وتكوين الصداقات الافتراضية التي ولدت للمجتمعات العربية عامة والمجتمع العماني بصفة خاصة الكثير من المشكلات الاجتماعية والتي عرضت أفراده للاحتيال والتصيد والتلاعب النفسي وتعرضه للمطاردة أو ضحايا لبعض جرائم الاستغلال العاطفي والجنسي، بل ازداد الأمر ليشمل الإصابة ببعض اضطرابات ما بعد الصدمة نتيجة وقوع المرء كضحية لتلك النوع من الجرائم نتيجة انتهاك خصوصية الفرد وعدم التفاعل الحي المرئي بين طرفي الاتصال وانتحال الهوية وغموض هوية المتصل من مستخدمي منصات التواصل الاجتماعي ووسائل التواصل الإلكتروني، ومع تلك التطورات التكنولوجية ظهرت أشكال جديدة من الجرائم تستهدف هذه المنصات، وتُعرف بالجريمة السيبرانية القائمة على منصات التواصل الاجتماعي.

يستخدم مصطلح الجرائم السيبرانية لوصف انتشار النشاط الاجرامي في الفضاء السيبراني، وهي مكمل للجريمة التقليدية إذ يعتمد على شبكات الانترنت للترويج للأنشطة غير المشروعة، أو تضليل الوعي المجتمعي ونشر الشائعات الخاطئة، او الوقوع ببيانات عسكرية في أيدي جهات اجنبية أو غيرها من تلك الانتهاكات السيبرانية (Das & Nayak, 2013). وفي تقرير صدر عن الحكومة في المملكة المتحدة عن تكلفة الجرائم السيبرانية والتي بلغت 27 مليار جنيه إسترليني أي ما يعادل 1.8٪ من الناتج المحلي تراوحت بين خسارة المواطنين والشركات والحكومة، بالإضافة إلى سرقة الملكية الفكرية للشركات والتجسس (Anderson et al., 2013). وقد يكون من دوافع ارتكاب الجريمة السيبرانية هي المتعة، أو بدافع إرضاء الأنا، وقد تكون لإشباع دوافع أيدولوجية، او سياسية، أو بدافع الكراهية، أو لكسب الأموال والربح (Das & Nayak, 2013).

http://dx.doi.org/10.29009/ijres.7.3.1

يهدف هذا البحث إلى إجراء دراسة استكشافية للوقوف على ظاهرة الجريمة السيبرانية القائمة على منصات التواصل الاجتماعي في المجتمع العماني، وذلك من خلال تحليل أنماط وأشكال هذه الجرائم، وتحديد التأثيرات الاجتماعية والنفسية والاقتصادية على الأفراد والمجتمع بشكل عام. وتعتمد المنهجية المستخدمة في هذا البحث على الاستكشاف، حيث يتم مراجعة الأدبيات المتاحة في هذا المجال وإجراء مقابلات مع متخصصين في مجال الجريمة السيبرانية، بالإضافة إلى أفراد من المجتمع العماني الذين تعرضوا للأذى من هذه الجرائم أو يشتبه في تورطهم في ارتكابها. سيتم تحليل البيانات المجمعة بشكل كمِّي ونوعي لاستخلاص الاتجاهات والأنماط والعوامل المؤثرة.

مفهوم الجريمة السيبرانية

تعرف بأنها الجرائم التي تتراوح بين النشاط الاجرامي ضد البيانات وانتهاك المحتوى وحقوق الطبع والنشر، وتتضمن بعض الأنشطة منها الاحتيال، والوصول غير المصرح به، والمواد الإباحية عن الأطفال، والمطاردة عبر الانترنت (Das & Nayak, 2013). وأضاف Bossler & Berenblum (2019) إليهم العنف السيبراني المتمثل في المطاردة والإرهاب السيبراني. وتتراوح جرائم الاحتيال الالكتروني بين الاحتيال على البطاقات الائتمانية، أو الاحتيال المروج له من العصابات ومافيا الادوية لبيع الأدوية المزيفة، وإدارة شبكات الروبوتات (Anderson et al., 2013).

كما يمكن تعريف الجريمة السيبرانية اجرائياً أنها جريمة تعتمد على التقنيات الرقمية لارتكاب الجريمة، وتحمل الجريمة في طياتها خطاب الكراهية أو التنمر أو الايذاء الالكتروني، ويكون نص الخطاب مغلفا بنطاقات كتابية متضمنة نوع من أنواع الكراهية أو لغة تحمل العنف والعنصرية (Gambhir et al., 2022). وغالبا تحدث الجرائم السيبرانية نتيجة افتقاد مستخدمي

http://dx.doi.org/10.29009/ijres.7.3.1

مواقع التواصل للأمن السيبراني والوعي السيبراني، وانسياقهم وراء المشاعر التي قد تزفها الشائعات دون التحقق من مصادر تلك المعلومات ويقع الفرد ضحية لنشر تلك الشائعات فيجد نفسه معرضا للحساب تحت طائلة القانون (Khandelwal & Chaudhary, 2022). وتشترك هذه الأنواع من الجرائم مع الجريمة التقليدية في أنها تستخدم التزوير والاحتيال، ونشر محتويات غير قانونية عبر مواقع التواصل الاجتماعي كمواد الاعتداء الجنسي على الأطفال أو التحريض على الكراهية والعنصرية، وتختلف الجريمة السيبرانية في محتواها عن نظيرتها التقليدية في أنها غير محددة الهوية لمرتكبها، وعدم وجود حدود او نطاق لمسرح الجريمة، واعتمادها المسبق على تفاعلات في الواقع الحي ونقله الكترونيا بدافع الانتقام (Anderson et al., 2013). ويمكن تقسيم الجريمة السيبرانية إلى فئتين من حيث الطبيعة الاجرامية وهما (Gordon & Ford, 2006):

1) الجرائم السيبرانية ذات الطبيعة التكنولوجية.
2) الجرائم السيبرانية التي تحتوي على عنصر بشري أكثر وضوحاً.

خصائص الجريمة السيبرانية

أشارت دراسة (Rosa et al., 2019) أن من خصائص الجرائم السيبرانية مايلي:

1- توافر نية الايذاء.
2- وتكرار السلوك العدواني مع مرور الوقت.
3- عدم توازن القوى بين المجرم والضحية.
4- أنها عمل عدواني متعمد يقوم به شخص أو جماعة في الفضاء السيبراني.

كما أضاف (Selkie et al., 2016) أن من خصائصها أنها سلوكيات حتمية الضرر على الضحية، بينما أضاف (Berne et al. ,2013) إلى أنه خلل ملحوظ أو مدرك في القوى ويتكرر عدة

http://dx.doi.org/10.29009/ijres.7.3.1

مرات وبالتالي يتصف أنه يكون متناوب، وغالبا يحتدم الصراع ويصل إلى حد الجريمة نتيجة غياب بعض السمات عن البيئة الحية مثل: نغمة الصوت وتعبيرات الوجه، ونقص الوضوح والشفافية. وأضاف (Whittaker & Kowalski ,2015) شرط حدوث الجرائم السيبرانية الموجهة نحو الأفراد وجود اختلافات في القوة البدنية أو الوضع الاجتماعي والخبرة التكنولوجية. في حين أكد Whittaker & Kowalski (2015) أن من خصائص الجرائم السيبرانية مجهولية المجرم مرتكبي الجرائم ويكون تصيد الأشخاص غرضه عرقيا أو دينياً أو مهنياً.

أبعاد الجريمة السيبرانية

1- **تطور المجال العلمي Development of the Scientific Field**: حيث يرتبط بعوامل خارجية مثل التمويل والبني التحتية والتعليم العالي والثقافات الاكاديمية المحلية (Liu et al., 2012).

2- **الاستقلالية أو التبعية Autonomy/Dependency**: تتعلق بعدة شروط منها وجود علم الاجرام أي بُعد الاستقلالية أو التبعية، ويحتوي علم الاجرام على القدرة على نمو الجريمة والاستقلالية (Liu et al., 2012).حيث تشير الاستقلالية إلى قدرة المهاجمين على تنفيذ أنشطتهم السيبرانية الضارة بشكل مستقل وبدون تبعية أو ربط مباشر بأطراف أخرى. ويمكن تفسير ذلك أن المهاجمين قادرون على تخطي القيود والرقابة والتعقب التي تفرضتها الحكومات والهيئات الأمنية والقانونية، وبالمقابل تشير التبعية إلى الربط أو الاعتماد على أطراف أخرى في تنفيذ الجريمة السيبرانية. قد يكون هناك تبعية للمهاجمين لأطراف مثل المنظمات الإجرامية المنظمة، أو الدول، أو الجماعات الهاكر المنظمة.

http://dx.doi.org/10.29009/ijres.7.3.1

3- **المركزية والتهميش Centrality/Marginality**: فقد يكون هناك سبب وراء استهداف شركة معينة ليس للاستيلاء على المال، وإنما للسيطرة على بيانات أشخاص بعينهم، أو لبيع هوية العملاء، أو بغرض الملاحقة، أو التورط في الانتقام؛ وبالتالي فهذا يؤكد دوافع الربحية والايدولوجية (Broadhurst & Chang, 2012). وتشير المركزية إلى تركيز القدرات والموارد والمهارات والاستخدام الفعال للتكنولوجيا في أيدي مجموعة محدودة من الأطراف في مجال الجريمة السيبرانية حيث أن بعض الأفراد أو المؤسسات قد تكون لديها قدرات تقنية وموارد مالية أكبر تمكنهم من تنفيذ هجمات إلكترونية متقدمة ومدمرةوقد يمتلكوا أحدث التقنيات والأدوات والمعلومات، في حين يكون لدى الأطراف الأخرى موارد وقدرات محدودة لمكافحة الجريمة السيبرانية، أما التهميش، فهو يشير إلى الحالة المعاكسة، حيث تكون لدى بعض الأطراف قدرات وموارد وفرص محدودة للدفاع عن نفسها أو مواجهة الهجمات السيبرانية.

أنماط وصور الجريمة السيبرانية

أولاً: جريمة التنمر السيبراني: وتتم من خلال وسائل التواصل الاجتماعي بين الشباب والكبار، وهذا النوع من الجرائم تتأثر بالسمات الشخصية لكلا من المتنمر والضحية، وكذلك انخفاض الرضا بالحياة ويميل الضحية للتفكير الانتحاري في بعض الأحيان (Giumetti & Kowalski, 2022). وتحكم هذه الظاهرة من الناحية النفسية ظاهرة الازدواجية أُثناء ممارسة التسلط أو التنمر، فالفرد ينتهج سلوكين، أو دورين متضادين إما متنمر الكتروني، أو كونه ضحية الكترونيا في نفس الوقت. وغالباً يقع الاناث ضحية لهذه الجريمة بسبب الافتقار إلى اتباع القواعد السليمة في التفاعل، بالإضافة إلى نوع التربية التحررية التي تنتهجها أسرة الضحية (Lozano-Blasco,

http://dx.doi.org/10.29009/ijres.7.3.1

(et al., 2020. بالإضافة إلى الغياب الزماني والمكاني لحدوث تلك الجريمة كان سببا وراء انتشارها ونقص اشراف البالغين (Selkie et al., 2016). وتتراوح هذه الجريمة بين مقاطع الفيديو المهينة والملاحظات السيئة، والتحرش من خلال التعليقات الخبيثة عبر شبكات التواصل الاجتماعي (Rosa et al., 2019). حيث يكون الغرض الأساسي اذلال الضحية، ومهاجمة واستبعاد شخص عاجزًا نسبياً (Rosa et al., 2019).

ثانياً: جريمة الملكية الفكرية المرتبطة بالذكاء الاصطناعي: حيث تعتمد هذه الجرائم على انتهاكات تختص بالكتابات العلمية الأصيلة، والتي تسبب في انتاج معرفة علمية دون تجريب الأمر الذي يؤدي الصدق التعميمي له إلى كارثة خاصةً في المجال الطبي، وتعتمد هذه الجرائم على برامج الذكاء الاصطناعي ومواقع روبوتات الدردشة سابقة الاعداد اللفظية والتي تعتمد على خاصية معالجة اللغة الطبيعية في مجال الذكاء الاصطناعي، والتي ترتكز على توليد نصوص وتفسيرات تحاكي تلك البشرية اعتمادا على التعلم العميق وألية معالجة اللغة الطبيعية NLP والتي توحد الكلمات بالبحث في الويب السيمانتي اعتمادا على خوارزميات للحصول على جمل ذات معنى يتم التعبير عنه بإيجاد تشابهات وتقديم تفسيرات وتعبيرات تبدو منطقية وإيجاد تراجم صوتية أحيانا (Ramírez Sánchez et al., 2021). وفي الفترة الأخيرة تطورت روبوتات تعتمد على تقنية التعلم العميق لاستخراج المعلومات الدلالية التي تنشر عبر صفحات منصات التواصل الاجتماعي والتي تنتهك الأعراف والقوانين والتي يدخل مروجوها تحت طائلة القانون (Kumari et al., 2018).

ثالثاً: القضايا السياسية السيبرانية: وهي وسيلة تستخدمها الدول المعادية لحشد الرأي العام في غياب الرقابة الأمنية كما هو في بعض الدول، وغالبا تكون تلك الأراء والحشود لتخريب وتحطيم الخطاب الجماهيري والاستقطاب الاستباقي لاختلاق خداع السيطرة، والتأثير على

http://dx.doi.org/10.29009/ijres.7.3.1

الرأي العام واستقرار البلاد وإثارة مشكلات اقتصادية (Gunitsky, 2015)، ويكون غرض تلك الجرائم (Gunitsky, 2015): التعبئة المضادة، تأطير الخطاب لتغيير إدراك الجمهور، والكشف عن التفضيلات، وتنسيق النخبة أو قد يكون هناك صور أخرى مثل استخدام غسيل المخ باسم المواطنة الرقمية والتحول الجذري نحو السعي لكوكب متحضر للترويج للعديد من الأفكار الهدامة في مجتمع معين لقتل الهوية الثقافية واللغوية والحضارية (Arribas-Bel et al., 2015). وقد تطورت تقنيات الذكاء الاصطناعي لتتبع تلك الجرائم وتصيد مروجي تلك النصوص أو مرتكبي السلوك الضار وغير القانوني (Velasco, 2022).

رابعاً: جريمة الهجمات السيبرانية Cyber attack: وتحدث هذه الجريمة كرد فعل على حادث اجتماعي يتضمن مناقشة هائلة على وسائل التواصل الاجتماعي (Mandal et al., 2020). وتتراوح بين القرصنة السيبرانية (Shu et al., 2018). وغالبا تحدث هذه الجرائم نتيجة العديد من التحديات منها (Shu et al., 2018):

- تحدي البيانات والتي غالبا ما تعتمد على البيانات التي ترتبط بالمشاعر.
- تحدي الميزات عن طريق استخراج المميزات الفعالة والقوية من منشورات وسائل التواصل الاجتماعي القصيرة والصاخبة. ولاقت هذه الجريمة رواجًا نتيجة عدم القدرة على كشف هوية المهاجم وغموض بيانات الشبكة التي يتم اختراقها داخل المؤسسة (Sliva et al., 2019).

خامساً: جريمة الابتزاز العاطفي والتحرش الالكتروني Emotional Blackmail and Cyber harassment: تتضمن هذه الجريمة الانخراط في فعل أو سلوك تعذيب شخصاً أو ازعاجه أو ترهيبه أو إهانته أو تهديده أو استغلاله جنسياً أو عاطفياً عبر البريد الإلكتروني أو عبر مواقع التواصل الاجتماعي بهدف احداث الأذى (Hazelwood & Koon-Magnin,

http://dx.doi.org/10.29009/ijres.7.3.1

(2013. وتتراوح بين الأفعال المهينة والتهديدية التي تعبر عن التحرش الصريح البادي بالاهانات اللفظية والايحاءات والاعتداءات الجنسية المصورة، وغالبا يصنف هذا النوع من العداء العلائقي، ويشير Beran & Li (2005) إلى الاستبعاد من نشاط ما ونشر الشائعات لوصم شخص ما بجريمة جنسية ما، أو عن طريق السب الصريح، أو الدفع أو سرد تفاصيل وقصص وسيناريوهات غير صحيحة الكترونياً. وغالبا ما تكون تلك الجرائم موجهة تحديداً نحو الأطفال لسبب سيكولوجي إذ أن الطفل يستسلم لا ارادياً للمعتدي عن طريق البكاء أو الانكماش والتراجع، وحينها يظهر المعتدي قوته وهيمنته على الضحية، وحينها ترضخ الضحية بالتبعية غير تطوعية إلى الاكتئاب والعجز (Beran & Li, 2005; Li, 2005).

نظرية تناوب السيطرة

تعتبر إحدى نظريات علم النفس الجنائي التي قام بتطويرها Moussa (2020a) وهي تفسر طبيعة السلوك العدائي، وتقوم على فرض أن العداء نهاية حتمية في نهاية المواقف الحياتية للمرء. وتتدرج النظرية في وصف التنمر الاجتماعي؛ إذ تفترض وجود طرف متسلط يتصف ببعض السمات الشخصية النرجسية من ذوي تقدير الذات المنخفض ويعتمد في تسلطه على الآخرين أو تنمره عليهم على طرف خارج عن إطار الموقف يتصف بشخصية عصابية في فرض سيطرة المتسلط الانفعالية على الآخرين، وتفترض عمليات التسلط وجود طرف ضعيف يمكنه الرد ثأراً لحقه ولكن ليس بالقوى التي يمتلكها الآخر.

وتبدأ الجريمة باستدراج الضحية للضحية للوصول إلى مصلحة مزعومة تمكنه من زيادة اعتقاده بقوة الأنا لديه، والاحساس بالذات بصورة مبالغاً فيها، خصوصاً وأن هذا الطرف الضعيف غير معطياً لهذه السيطرة، وتشعر الضحية بالانقياد وغلبة الأمر إلى أن تشعر بتكافؤ القوى، وحين ذلك يستخدم الضحية نقاط ضعف الشخصية النرجسية للمتسلط لتحقيق

http://dx.doi.org/10.29009/ijres.7.3.1

تناوب السيطرة، وهنا يستخدم إحدى الطريقتين: إما تحطيم المتسلط نفسياً، أو مجاراته للوصول به إلى نقطة انهيار قد تكون فخاً. وعادة إذا كانت سمات الشخصية قوية لدى الضحية فإنه ينتظر الوقت الذي يمتلك فيها القوة للرد على المتسلط لتحطيمه انفعالياً أمام الاخرين. وتتكون النظرية من العديد من المراحل منها:

1. تحديد نقاط القوة لاستغلالها لدى الضحية، ونقاط الضعف ورصدها واستخدامها كثغرة للتأثير على الضحية إما عن طريق الابتزاز أو الاستدراج أو الاستقطاب أو الاستمالة.
2. استخدام قوة الضغط ثم التهكم التنظيمي للضغط على الضحية فيصبح أمام حدود التأطير، إما فعل كذا أو ينزل عليه الإيذاء.
3. استمرار عمليات التهكم التنظيمي عند ملاحظة تفوق الضحية في أحد سمات الشخصية كنوع من الضغط لخفض تقدير الذات لديه.
4. الوصول إلى نقطة الانهيار للضحية بتخطي حدود وصيد التحمل، فيتحول الضحية إلى شخصية استغلالية تجعلها انتقامية دون دراسة نتائج سلوكياتها.
5. مرحلة الشلل الانفعالي والتي يصل إليها النرجسي لعدم توقعه رد الفعل العنيف من الضحية بالقدر الذي جعله معرى الذات أمام الآخرين، فهو لا يستطيع الرد لانعكاس التهكم التنظيمي عليه بالصورة التي جعلته ضعيفاً أمام كل الشخصيات التي تنمر أو تسلط عليها.

http://dx.doi.org/10.29009/ijres.7.3.1

6. مرحلة الانطواء وفيها يأخذ المتسلط الذي تحول لضحية جانباً لينعزل عن الآخرين. وهنا يفترض مؤلف النظرية أنها تسير عكس جميع قواعد التسلط بشتى أنواعه فقد تتحول الضحية إلى مستغل، ولكن لا يتحول المتسلط إلى ضحية.

مشكلة الدراسة

عانت دول مجلس التعاون لدول الخليج العربية في الفترة الأخيرة من انتشار الجريمة السيبرانية الموجهة نحو الأفراد، والجرائم السيبرانية المتصلة بالتنمر الالكتروني، حيث ظهرت العديد من الجوانب التي لم يتم الإبلاغ عنها من الجرائم الالكترونية منها جرائم الاستغلال العاطفي والابتزاز الالكتروني وجرائم الملاحقة والمطاردة التي أفرزتها الدراسات في مجال علوم الجريمة ومجال أمن المعلومات، ولكن مجال علم النفس لم يكن بالصورة الخصبة لتبني مثل تلك النوع من الجرائم، وفي ضوء انتشار تطبيقات الذكاء الاصطناعي وما تبعته من جرائم متطورة الكترونية زادت من تفاقم الكشف عنها حيث أنها تنتج محتويات الكترونية أصيلة ويتم تسجيلها كملكية فكرية ومع تطور أدوات الكشف عن الانتحال يتم كشفها، أو من خلال انتاج برامج انتاج محتويات صوتية أو مرئية اعتمادا على نغمات وطبقات الصوت، وظهرت المحاكم الاقتصادية في بعض الدول العربية لمكافحة مثل تلك الأنواع من الجرائم السيبرانية، وبالرغم من هذا العدد المتنامي من الجرائم إلا أنها لم يفصح عنها في البحث العلمي.

ونظرا لصرامة القوانين في البيئة العمانية لمكافحة هذا النوع من الجرائم ومرتكبيها إلا أن الضحايا هذه الجرائم لم يبلغوا عنها خوفاً من نظرة المجتمع ونظرا لشعورهم بالخزي والعار من الإبلاغ عن وقوعهم كضحايا أمام المجتمع العماني خوفا من الرواج الإعلامي نتيجة غرابة محتوى الجرائم. ونظرا لحساسية الظاهرة المقاسة فتطرح الدراسة الموضوع بطريقة تبرز وعي المجتمع العماني بالوعي بالجريمة السيبرانية المعتمدة على منصات التواصل الاجتماعي نظراً

http://dx.doi.org/10.29009/ijres.7.3.1

لكثرة الضرر الواقع منها. ولم يقف الأمر عند هذا الحد بل تجاوز الأمر في الفترة الأخيرة توابع حروب الجيل الخامس من نشر الشائعات والتلاعب بعقول الشباب والأطفال، وبالتالي جاءت الدراسة للوقوف على مستويات الوعي باعتباره مؤشراً للوعي السيبراني.

ومن الملاحظ أنه توجد عوامل نفسية وشخصية تؤثر على وقوع المرء كضحية للجرائم السيبرانية منها انسيابية التعبير عن الذات، وهشاشة الأنا، وشعور المرء بالاغتراب النفسي والاجتماعي، ومثالية التفاعلات التي ترتبط بالأنا المثالية أو مزيج بينها وبين الأنا الاجتماعية، كم أن التقمص العاطفي والتلاعب بالافكار والعواطف والمشاعر، خصصا وأن المرء يدخل إلى منصات التواصل الاجتماعي وقت الخوف أو شعوره بالاكتئاب والوحدة النفسية وبالتالي يجعله التوتر والخوف عرضة لتصديق الإيحاء البادي إليه في حدة تفاعلاته مع الاخرين أو المحتوى بل ويتعدى الأمر حد الاستغراق الانفعالي (Bhandari & Bimo, 2020; Fakhrou et al., 2022; Gálik, 2019; Kirwan, 2016; Kurniawan, 2018; Suler, 2002; Zuo & Wang, 2019)، بل والصدمة العاطفية إذا لم يقع المرء ضحية للابتزاز العاطفي الكترونياً (Moussa, 2020a,b). ويمكن تناول مشكلة الدراسة الحالية في التساؤلات التالية:

1) ما أفضل بناء عاملي ينتظم حولها مفردات مقياس الوعي المدرك للجريمة السيبرانية المرتبطة بمنصات التواصل الاجتماعي في المجتمع العماني؟
2) ما مدى وجود فروق ذات دلالة إحصائية في الوعي المدرك للجريمة السيبرانية المرتبطة بمنصات التواصل الاجتماعي باختلاف الجنس والمؤهل الدراسي والخبرة الوظيفية ونوع الإقامة ومحل الإقامة لدى الفرد العماني؟

أهداف الدراسة

تهدف الدراسة إلى التحقق من:

http://dx.doi.org/10.29009/ijres.7.3.1

1) دراسة البنية العاملية التي ينتظم حولها مفردات مقياس الوعي المدرك للجريمة السيبرانية المرتبطة بمنصات التواصل الاجتماعي.

2) دراسة الفروق في الوعي المدرك للجريمة السيبرانية المرتبطة بمنصات التواصل الاجتماعي باختلاف الجنس والمؤهل الدراسي والخبرة الوظيفية ونوع الإقامة ومحل الاقامة.

أهمية الدراسة

تسعى الدراسة إلى استكشاف مدى الوعي المدرك لطبيعة الجريمة السيبرانية المتصلة باستخدام منصات التواصل الاجتماعي في المجتمع العماني وخاصةً الجرائم المتصلة بالرأي العام أو الجرائم المتصلة بالذكاء الاصطناعي. والتطلع في ضوء النتائج وضع برامج للتوعية المجتمعية بمخاطر الجريمة السيبرانية وأنواع التفاعل التي قد ينساق بها الفرد العماني وراء أحلام توقع به كضحية للمساءلة القانونية.

حدود الدراسة

يمكن تعميم نتائج الدراسة على نطاقات أوسع، مع الحرص البالغ في تعميم نتائج العينة على الزائرين والمقيمين في سلطنة عمان حيث إن عددهم لم يتخط 11٪ من إجمالي العينة، بالإضافة إلى عدم قدرة الدراسة على تعميم النتائج على نطاقات أوسع من الطلبة والأفراد بدون عمل حيث أن العينة لم تتخط 11٪ هي الأخرى حتى لا يكون هناك تحيزاً في صناعة القرار. حيث طبقت أداة الدراسة في الفترة من 16 نوفمبر 2022 حتى 19 أكتوبر 2023 وذلك باستخدام الاستبانة الالكترونية.

الطريقة والاجراءات

http://dx.doi.org/10.29009/ijres.7.3.1

أولاً: المشاركون

تكونت عينة الدراسة من 170 من أفراد المجتمع العماني حيث اختيرت عينة الدراسة بطريقة كرة الثلج. وقد كان تصنيف العينة في ضوء المتغيرات الديموغرافية على النحو التالي:

جدول (1): تصنيف العينة في ضوء المتغيرات الديموغرافية لعينة الدراسة من المجتمع العماني

Table (1): Sample classification according to demographic variables for the Omani community patrticipants

المتغير	مستويات	التكرار	النسب المئوية
المؤهل الدراسي	دكتوراة	5	٪3
	ماجستير	31	٪18.2
	بكالوريوس	117	٪68.8
	دبلوم تأهيلي	17	٪10
النوع الاجتماعي	ذكور	46	٪27.1
	اناث	124	٪72.9
الخبرة الوظيفية	10 سنوات فأكثر	35	٪20.6
	أقل من 10 سنوات	17	٪10
	موظف	100	٪58.8
	بدون عمل	11	٪6.5
	طالب	7	٪4.1
نوع الاقامة	مواطن	150	٪88.2
	مقيم	18	٪10.6
	زائر	2	٪1.2
محل الاقامة	شمال الباطنة	27	٪15.9
	جنوب الباطنة	14	٪8.2
	مسقط	37	٪21.8
	الداخلة	12	٪7.1

http://dx.doi.org/10.29009/ijres.7.3.1

المتغير	مستويات	التكرار	النسب المئوية
	شمال الشرقية	9	٪5.3
	جنوب الشرقية	12	٪7.1
	الظاهرة	6	٪3.5
	البريمي	4	٪2.4
	ظفار	48	٪28.2
	مسندم	1	٪0.6

وقد تم الحصول على استجابات العينة من خلال الاستجابة السيبرانية، وقد أعلن الغرض من إجراء الدراسة للعينة كي يمكن للعينة الاستجابة بعد فهم طبيعة الاجراء، ويمكن للعينة الانسحاب وقتما يشاء حينما يجد أن الإستجابة لأداة الدراسة تتعارض مع مصلحته الشخصية أو عند شعوره بالملل.

ثانياً: مقياس الوعي المدرك للجريمة السيبرانية المرتبطة بمواقع التواصل الاجتماعي

تكون المقياس من 16 عبارة تقريرية للوقوف على مدى وعي المجتمع العماني بالجريمة السيبرانية وبعض مظاهرها السلوكية التي يتم ارتكابها في منصات التواصل الاجتماعي. وقد تم الاستفادة من بعض الدراسات السابقة التي تناولت أنواع معينة من الجرائم السيبرانية ومنها (Anderson et al., 2013; Beran & Li, 2005; Giumetti & Kowalski, 2022; Gordon .& Ford, 2006; Ramírez Sánchez et al., 2021; Sliva et al., 2019; Velasco, 2022)

وقد صيغت استجابات العبارات في ضوء مقياس ليكرت الثلاثي بحيث تعطى استجابة موافق 3 درجات، بينما محايد تعطى درجتين، وتعطي استجابة غير موافق درجة واحدة. وقد تم اختيار مقياس ليكرت الثلاثي لتضييق فجوة اتخاذ الرأي خصوصاً وأن المصطلحات الواردة والمعبرة عن تلك النوع من الجرائم السيبرانية المرتبطة بوسائل التواصل الاجتماعي قد تكون غير مدركة،

http://dx.doi.org/10.29009/ijres.7.3.1

وبالتالي لزاماً أن تكون فجوة الاستجابة ضيقة. وقد صيغت العبارات بصيغ إيجابية غير منفية لتجنب الغموض.

ثالثاً: التحليل الاحصائي

استخدام برنامج Jamovi 2.3.26 لإجراء التحليل الاحصائي وذلك بحساب مؤشرات الإحصاء الوصفي كالتكرارات والنسب المئوية لتوصيف العينة، بالإضافة إلى استخدام التحليل العاملي الاستكشافي للتعرف على بنية المقياس وتحديد عدد العوامل المكونة للمقياس. كما استخدم التحليل العاملي التوكيدي للتحقق من مدى مطابقة هذه العوامل المكونة للمقياس لطبيعة العينة. وقد حساب الثبات باستخدام معامل ألفا كرونباخ ومعامل ماكدونالد أوميجا.

رابعاً: إجراءات الدراسة

تم الاطلاع على الدراسات السابقة للتعرف على الجوانب التي ترتبط ببعض الجرائم السيبرانية، ونظراً لقلة شيوع مثل هذه الجرائم في المجتمع العماني فقد حاول الباحثون في هذه الدراسة صياغة العبارات بصورة ترتبط بالوعي بنوعية الجرائم السيبرانية المرتبطة بمنصات التواصل الاجتماعي. وقد تم تحكيم أداة الدراسة من حيث الصياغة وسلامة العبارات وتم إجراء التعديلات قبل تطبيقها. كما أنه تم صياغة المقياس بصورة الكترونية في منصة جوجل فورم. وقد أطلق ميثاق الموافقة المستنيرة لمستجيبي العينة وتعريفهم بحقوقهم وواجباتهم، وقد استمرت فعاليات التطبيق من 16 نوفمبر 2022 حتى 19 أكتوبر 2023. وقد كانت الاستجابة على الأداة دون التطرق لأي تفاصيل شخصية كالاسم أو الهوية حتى لا يتم تزييف الاستجابة.

http://dx.doi.org/10.29009/ijres.7.3.1

نتائج الدراسة وتفسيرها

أولاً: الصدق البنائي لمقياس الوعي المدرك للجريمة السيبرانية المرتبطة بمواقع التواصل الاجتماعي

تم استخدام التحليل العاملي الاستكشافي للتعرف على البناء العاملي الذي تنتظم حوله مفردات المقياس، وقد استخدمت الطريقة الافتراضية للبرنامج وهي Minimum residuals والتدوير المائل بطريقة Oblimin وقد تركت المفردات حرة دون تحديد عدد العوامل التي يستخلص حولها مفردات المقياس. وكانت مؤشرات المطابقة على النحو المبين:

جدول (2): مؤشرات حسن المطابقة لنموذج التحليل العاملي الاستكشافي لأداة الدراسة.

Table (2): Goodness of fit Indicators of the exploratory factor analysis of the study instrument.

المؤشر	p	df	X2	TLI	RMSEA	KMO
القيمة	0.001	120	1681	0.904	0.085	0.906

اسفرت النتائج عن مطابقة حسنة فقد بلغت قيمة مؤشر كايزر ماير أولكين (0.906) مما يعني مناسبة العينة لإجراء التحليل، وكان محك التماثل لبارتليت دال احصائياً، بينما حقق مؤشر TLI مطابقة حسنة، فيما أن مؤشر RMSEA كان متضخماً لكنه لم يتخط القيمة المقبولة.

وأفرز التحليل العاملي الاستكشافي عاملين فسرا 53.1٪ من التباين الكلي للظاهرة، وقد كانت الجذور الكامنة للعاملين على الترتيب 6.79 و1.46 وفُسرت العوامل 36.2٪ و16.8٪ من التباين الكلي للظاهرة، وتم ملاحظة أن الجذر الكامن للعامل الأول متضخماً وهو العامل الذي يعبر عن الجرائم المجتمعية المرتبطة بمواقع التواصل الاجتماعي، بينما العامل الثاني يرتبط بالجرائم الفردية المرتبطة بمنصات التواصل الاجتماعي. وقد كانت تشبعات المفردات على نموذج العاملين على النحو المبين:

http://dx.doi.org/10.29009/ijres.7.3.1

جدول (3): تشبعات مفردات مقياس الوعي المدرك للجريمة السيبرانية المرتبطة بمواقع التواصل الاجتماعي على العاملين.

Table (3): Item Loadings of for the awareness of cybercrime related to social networking sites on the two factors.

م	العوامل		الشيوع
	العامل الأول	العامل الثاني	
1	0.88		0.30
6	0.87		0.23
11	0.85		0.25
4	0.85		0.27
15	0.84		0.30
9	0.83		0.23
2	0.83		0.34
12	0.76		0.39
13		0.71	0.56
10		0.65	0.54
5		0.64	0.62
7		0.58	0.61
16		0.57	0.59
14		0.53	0.67
3		0.44	0.75
8		0.32	0.88

تراوحت تشبعات الجرائم المجتمعية التي ترتبط بالمنصات التواصل الاجتماعي بين 0.76 إلى 0.88 بمتوسط حسابي 0.84، بينما تراوحت تشبعات بعد الجرائم الفردية المرتبطة بمنصات التواصل الاجتماعي بين 0.32 إلى 0.71 بمتوسط حسابي 0.56.

http://dx.doi.org/10.29009/ijres.7.3.1

أجري التحليل العاملي التوكيدي للبنية المتولدة من التحليل العاملي الاستكشافي واختبار نموذج العاملين بالطريقة الافتراضية اقصى احتمال، وكانت مؤشرات حسن المطابقة على النحو المبين:

جدول (4): مؤشرات حسن المطابقة لنموذج الوعي بالجرائم السيبرانية المتصلة بمنصات التواصل الاجتماعي

Table (4): Goodness of fit Indicators of the awareness of cybercrimes related to social Networking platforms model

X^2	df	P	CFI	TLI	SRMR	RMSEA
226	103	0.000	0.925	0.912	0.051	0.083

أسفرت النتائج عن مطابقة حسنة فيما عدا مؤشر مربع كاي وذلك نظرا لحساسيته لحجم العينة وطبيعتها. وكانت تشبعات المفردات على العاملين على النحو التالي:

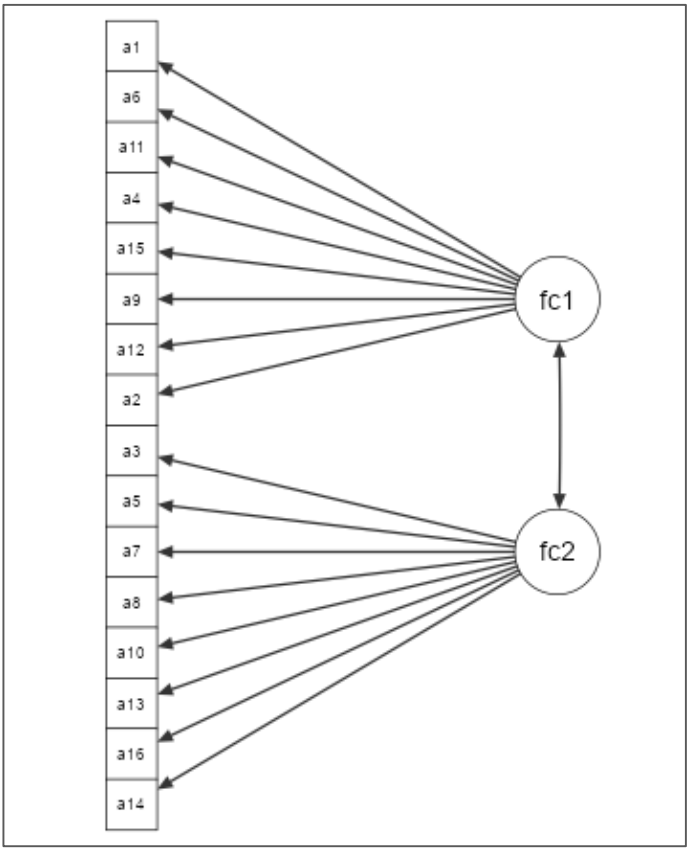
جدول (5): تشبعات مفردات مقياس الوعي بالجرائم السيبرانية المتصلة بمنصات التواصل الاجتماعي على العاملين.

Table (5): Item Loadings of the Cybercrime Awareness based on Social networking Platforms on the two factors.

البعد	م	التشبع	الخطأ المعياري	قيمة z	الدلالة
الوعي بالجرائم السيبرانية المجتمعية القائمة على منصات التواصل الاجتماعي	1	0.51	0.038	13.14	0.000
	2	0.56	0.044	12.72	0.000
	4	0.50	0.036	13.83	0.000
	6	0.57	0.040	14.47	0.000
	9	0.55	0.039	14.39	0.000
	11	0.56	0.040	14	0.000
	12	0.48	0.039	12.08	0.000
	15	0.53	0.040	13.38	0.000
الوعي بالجرائم السيبرانية الفردية القائمة على منصات التواصل الاجتماعي	3	0.30	0.045	6.54	0.000
	5	0.26	0.033	7.89	0.000
	7	0.41	0.049	8.31	0.000
	8	0.21	0.048	4.43	0.000
	10	0.46	0.049	9.36	0.000
	13	0.28	0.035	8.09	0.000
	14	0.30	0.041	7.41	0.000
	16	0.30	0.035	8.58	0.000

http://dx.doi.org/10.29009/ijres.7.3.1

تراوحت تشبعات المفردات في بعد الوعي بالجرائم السيبرانية المجتمعية القائمة على منصات التواصل الاجتماعي بين 0.48 إلى 0.57 بمتوسط حسابي للتشبعات بلغ قيمته 0.53، في حين تراوحت تشبعات المفردات في بعد الوعي بالجرائم السيبرانية الفردية القائمة على منصات التواصل الاجتماعي بين 0.21 إلى 0.46 بمتوسط حسابي لقيمة التشبعات بلغ 0.32 ولم تستبعد أي من مفردات الأبعاد. وقد كان الرسم التخطيطي للنموذج العاملي التوكيدي على النحو المبين:



شكل (1): النموذج العاملي التوكيدي لمقياس الوعي المدرك للجريمة السيبرانية المرتبطة بمواقع التواصل الاجتماعي

Figure (1): The Confirmatory Factor Analysis Model for the Perceived Awareness of Cybercrime based on Social networking Sites Scale

http://dx.doi.org/10.29009/ijres.7.3.1

كما تم حساب الثبات بطريقة ألفا كرونباخ ومعامل ماكدونالد أوميجا وقد بلغ الثبات للبعد الأول بطريقة ألفا 0.951 بينما بلغ معامل أوميجا 0.951 بينما بلغ الثبات للبعد الثاني بطريقة ألفا 0.792 بينما بلغ الثبات بطريقة أوميجا 0.802. وبلغ الثبات للمقياس ككل بطريقة ألفا 0.913 بينما بلغ الثبات بطريقة أوميجا 0.915.

ثانياً: مؤشرات الإحصاء الوصفي

حسب مؤشرات الإحصاء الوصفي والتشتت والشكل لأبعاد أداة الدراسة والدرجة الكلية وكانت النتائج على النحو المبين:

جدول (6): مؤشرات الإحصاء الوصفي لأبعاد أداة الدراسة والدرجة الكلية لعينة الدراسة.

Table (6): Descriptive Statistics Indicators of the Study Tool subscales and overall score

المؤشرات	الوعي بالجريمة السيبرانية	الجرائم المجتمعية	الجرائم الفردية
ن	170	170	170
القيم الغائبة	--	--	--
المتوسط	42.5	20.7	21.8
الوسيط	45	24	23
التباين	39.3	19.2	7.95
القيم الدنيا	18	8	10
القيم العظمى	48	24	24
الالتواء	1.32-	1.25-	1.85-
التفرطح	1.26	0.86	3.75
شابيرو ويلك (الدلالة)	0.832 (0.000)	0.755 (0.000)	0.774 (0.000)

جاءت درجات الوعي بالجرائم المجتمعية والجرائم الشخصية أو الفردية المرتبطة بمنصات التواصل الاجتماعي متقاربة من حيث قيم المتوسط مما يعني وعي الفرد العماني بتلك الجرائم والحيطة في التعامل مع الغرباء أو الأصدقاء في تفاعلات منصات التواصل الاجتماعي.

http://dx.doi.org/10.29009/ijres.7.3.1

بالإضافة إلى أن درجة التباين للوعي بالجرائم المجتمعية كان كبيراً إلى حد ما مقارنة بالوعي بالجرائم الفردية وهذا يشير إلى أن مدى الفروق الفردية متسعاً في الوعي بالجرائم السيبرانية الموجهة نحو المجتمع أي أن درجة الوعي متفاوتة فيما يتعلق بحقيقة الجرائم السيبرانية الموجهة نحو الاضرار بالمجتمع. في حين بلغ قيمة الالتواء لبعد الوعي بالجرائم الفردية أو الشخصية كان مرتفعاً وسالباً بما يعني أن الوعي المدرك من المجتمع العماني بالجرائم الموجهة نحو الأفراد عالياً بدرجة كبيرة ويعزي ذلك إلى الجهود المبذولة من شرطة عمان السلطانية لنشر الوعي السيبراني بتلك الجرائم وأضرارها الشخصية والمجتمعية.

ثالثاً: الفروق في الوعي المدرك للجريمة السيبرانية المرتبطة بمواقع التواصل الاجتماعي نتيجة تأثير المتغيرات الديموغرافية لدى المجتمع العماني

وللتحقق من تأثير المتغيرات الديموغرافية على أبعاد الوعي المدرك للجريمة السيبرانية المرتبطة بمواقع التواصل الاجتماعي تم استخدام اختبار تحليل التباين المتعدد المتدرج (هوتلنج ت)، وقد استخدم وظيفة Filter لانتقاء عينة من المجتمع العماني لدى نوع الإقامة لإجراء التحليل عليه. وكانت النتائج على النحو المبين:

جدول (7): نتائج تحليل التباين المتعدد المتدرج للفروق في الوعي بالجريمة السيبرانية (ن= 150)

Table (7): Results of the MMANOVA for Differences in Awareness of Cybercrime (n=150)

المتغيرات	هوتلنج ت	قيمة ف	دح1	دح2	الدلالة
المؤهل الدراسي	0.046	0.53	8	186	0.831
الخبرة	0.144	1.34	10	186	0.211
نوع الإقامة	0.064	1.49	4	186	0.206
محل الإقامة	0.147	0.76	18	186	0.746
النوع الاجتماعي	0.054	2.54	2	94	0.084

http://dx.doi.org/10.29009/ijres.7.3.1

أسفرت النتائج عن عدم وجود تأثير للمتغيرات الديموغرافية على أبعاد الوعي بالجريمة السيبرانية المرتبطة بمنصات التواصل الاجتماعي لدى المجتمع العماني.

وغالباً يكون النوع الاجتماعي غير مؤثراً على الوعي بالجريمة المرتبطة بمنصات التواصل الاجتماعي وقد يبرر هذا سببين الأول هو عدم وجود فروق في الوعي بسبب أن كلاهما لديه الوعي السيبراني، سواء بسبب التحفظ في تفاعلات افتراضية أو الاعتماد على المتابعة أو أن الوعي السيبراني بمصادر الخطر من بادئ الأمر متوفرة لدى أفراد المجتمع العماني، ومن ناحية أخرى التحفظ الزائد من المجتمع العماني بتجنب الاختلاط الافتراضي بين الجنسين، فالفرد ذكراً كان أو أنثى لا يقبل في صداقته إلا دائرة المعارف من نفس جنسه، الأمر الذي يجعل هناك وعي بطبيعة التفاعل المحدد بهدف إيجابي لا يجتر به بين براثن الأخطار الافتراضية، كما أن الوعي الافتراضي بالجريمة السيبرانية المجتمعية الموجهة نحو المجتمع عالياً يبدو في نسبة التباين المفسر في التحليل العاملي الاستكشافي حيث أن هذا العامل جذره الكامن كان كبيراً، ومن ناحية أخرى كان التباين المفسر لهذا البعد كان عالياً، وعلاوة على هذا فالجريمة الموجهة نحو المرء أي الجرائم الشخصية غير مدركة، حيث أن سببها هو تقبل أنواع من الصداقات مع الغرباء أو التفاعل مع الغرباء، أو أن الوعي السيبراني جعل أمام الفرد العماني حدوداً لا تقبل التداول في تخطيها بسبب صرامة القانون وبسبب الأعراف المجتمعية السائدة في المجتمع العماني.

كما أن نوع الإقامة أو محل الإقامة لا يؤثر في الوعي بطبيعة الجريمة السيبرانية المرتبطة بمنصات التواصل الاجتماعي، ذلك أن المواطن العماني وغير المواطن سواء أكان مقيم أو زائر يلتزم بالقانون ويمثل أمامه بالعقاب كل من يتخطى الحدود المسموح بها، وأن السيادة القانونية تقف حائلاً دون ارتكاب الجريمة السيبرانية سواء أكان بالتنمر أو بالتشهير والقانون صريحاً في هذا في رصد أي تخطي ومعاقبته، بالإضافة إلى هذا وطبقا لنظرية تناوب السيطرة فإن التفاعل

http://dx.doi.org/10.29009/ijres.7.3.1

الافتراضي للشباب والراشدين عبر مواقع التواصل الاجتماعي يلتزم في حدوده كلا من طرفي التفاعل، فالدافع للتواصل الاجتماعي هو متابعة الأخبار، أو متابعة نشاط اجتماعي موضع اهتمام، وبالتالي فتجاهل دخول مواقع التواصل الاجتماعي يجنب الشخص ظروف الهروب الاجتماعي كحيلة دفاعية من المشكلات الاجتماعية، حيث لا يتعرض المرء للاكتئاب بسبب الدخول إلى مواقع التواصل الاجتماعي، ويكون سبب الدخول إما المجاملة أو متابعة الأنشطة الاجتماعية، أو متابعة الحالة بصورة تجنب الشخص التصادم أو الابتزاز من قبل الغرباء.

كما أن القنوات الشرعية للتعبير عن الآراء داخل العمل مكفولة بحق القانون، فلا يحق لمستخدمي مواقع التواصل الاجتماعي التشهير أو التصريح بطريقة صريحة أو ضمنية عن شيء معين؛ بغرض الاعتراض على طريقة أو أسلوب إداري معين للمؤسسة التي يتعامل معها، إذ إن الوعي والسعي في الحصول على حقه بات بطريقة سهلة، وبالتالي يكون الوعي السيبراني في التعبير عن الآراء بطرق مقبولة، ولا يوجد ما يكفل للأفراد التهكم أو التنمر على زملائهم أو دائرة معارفهم. كما إن التعبير بنرجسية عن طبيعة الذات قد تبدو في صورة حب الذات بكثرة نشر الأخبار عن الذات للاعتزاز بالنفس أمام الأخرين أو لدواعي التفاخر بأنشطة مجتمعية قام بها الفرد، أو لتداول الذكريات بين مجموعة من الأصدقاء، وغالبا تكون مخصصة لمجموعة من الأصدقاء المقربين، وذلك امتثالا للوعي السيبراني خوفاً من التعرض للتنمر المدرك ممن حولهم، وبالتالي تجنب الخطر من تفاعلات الغرباء.

كما إن المرونة النفسية تكفل لمنتسبي المجتمع العماني سواء المواطنين أو المقيمين أو الزائرين التفاعل بمرونة دون الانخراط في أنماط مرهقة من التفاعل، حيث أن جرائم الأمن السيبراني التي يتم ارتكابها يتم ضبطها والتعامل معها بكل صرامة، وأن التفاعلات الافتراضية تكون بين دائرة الافراد المقربون وبالتالي فلا يشعر المرء بالغربة في تفاعلاته مع مزيج من الغرباء

http://dx.doi.org/10.29009/ijres.7.3.1

ممن يستنكرون تفاعلاته، خصوصا وأن التفاعلات الافتراضية مبهمة نتيجة افتقاد التواصل المباشر بين المرء ودائرة معارفه، وبالتالي لا يصل المرء لنقطة الانهيار في تفاعلاته التي تجعله ضحية للتنمر أو التشهير أو عرضة للامتثال أمام الادعاء العام لارتكابه الأخطاء.

المناقشة والتعليق

تناولت الدراسة محدد قوي وهو النوع الاجتماعي وبالأخص عينة الاناث التي كانت ثلاث أرباع العينة الكلية، حيث أنه قد يكون هناك نوع من التحفظ في الاستجابة على بيانات العينة، وذلك يرجع للطبيعة الثقافية المتحفظة للمجتمع العماني. وشملت الدراسة العديد من المحددات حيث أن العينة تضمنت العمانيين وغير العمانيين المقيمين بسلطنة عمان في الفترة الزمنية لتطبيق مقياس الدراسة، كما إن العينة غير ممثلة لجميع محافظات سلطنة عمان، وبالتالي فإدراك أو الوعي بالجريمة السيبرانية يختلف حسب النطاق الجغرافي، ولكن يمكن أن تعزى النتائج إلى أن ارتفاع الوعي السيبراني لدى عينة الدراسة مرتفعا بالدرجة التي يمكن أن تعمم بها نتائج الدراسة ولكن بحرص إذ أن عبارات مقياس الوعي بالجريمة السيبرانية فسرت 53.1٪ من إجمالي الوعي بهذا النوع من الجرائم، وعليه توصي الدراسة بعقد دورات تثقيفية لرفع مستوى الوعي السيبراني لدى المجتمع العماني.

كما اتضح من نتائج التحليل العاملي التوكيدي أن البناء مناسباً لطبيعة العينة في المجتمع العماني، ولكن هذا يعبر عن إدراك المرء ووعيه بطبيعة الجريمة المجتمعية أو الجريمة الفردية الموجهة نحو الفرد المرتبطة بمنصات التواصل الاجتماعي. وعلى الرغم من هذا فإن المتغيرات الديموغرافية لم تكن بدرجة أو بأخرى مؤثرة في طبيعة البناء، ومن ناحية سيكولوجية فإنه باختيار سكان عمان، باعتبارهم العينة الأكبر في متغير نوع الإقامة هو الأفضل بسبب أنها عينة كبيرة إلى حد ما، وحاولت الدراسة التغلب على بعض المحددات فقد جعلت الدراسة العينة

http://dx.doi.org/10.29009/ijres.7.3.1

بطريقة كرة الثلج بحيث يرسل أفراد العينة المقاييس إلى بعضهم البعض، وذلك لتلاشي تأثير البيانات الغائبة، أو للتغلب على الاستحسان الاجتماعي لدى المستجيبين على العينة. ومن منظور أخر يتضح من المستوى التعليمي أن العينة من طبقة مثقفة حاصلة على درجات علمية عالية مما يفترض أن الوعي السيبراني لديهم والوعي بالجريمة الالكترونية عالياً، ولكن النتائج قد تكون تعزي إلى أن عينة الحاصلين على بكالوريوس هي الأعلى عدداً وبلغت 117 فرداً، بالإضافة إلى أن باقي مستويات متغير المؤهل الدراسي تراوحت بين 5 إلى 17 فرد. وبالتالي لا يمكن تعميم النتائج فيما يختص بمتغير المؤهل الدراسي.

وقد توصلت الدراسة إلى أن تويتر هو منصة التواصل الاجتماعي الأشهر لدى المجتمع العماني وهي تختص بكتابة نصوص أو تويتات مصغرة أو مختصرة لإيصال الفكر بطرق راقية وطرق أكثر تأثيراً، وتعتبر منشورات تويتر أسهل من فيسبوك ذلك وأن مستوى الخصوصية ليس بنفس الدرجة الكافية لحماية المنشورات. كما أن التفاعلات تكون علنية مما يجعل المرء أمام العلن مكشوفة تفاعلاته مع الاخرين، وبالتالي يسودها السواء عما هو موجود في فيسبوك. لذا أوصت الدراسة بتمكين المواطنة الرقمية والانتماء باستخدام وسائل التواصل الاجتماعي، والاستمرار في تخصيص يوم وطني للأمن الإلكتروني في جميع المراحل التعليمية بالمؤسسات التربوية والتعليمية في سلطنة عمان وذلك لزيادة مستوى الوعي السيبراني بين جميع أفراد المجتمع العماني.

http://dx.doi.org/10.29009/ijres.7.3.1

References

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., ... & Savage, S. (2013). Measuring the cost of cybercrime. The economics of information security and privacy, 265-300.

Arribas-Bel, D., Kourtit, K., Nijkamp, P., & Steenbruggen, J. (2015). Cyber cities: social media as a tool for understanding cities. Applied Spatial Analysis and Policy, 8, 231-247.

Beran, T., & Li, Q. (2005). Cyber-harassment: A study of a new method for an old behavior. Journal of educational computing research, 32(3), 265.

Berne, S., Frisén, A., Schultze-Krumbholz, A., Scheithauer, H., Naruskov, K., Luik, P., ... & Zukauskiene, R. (2013). Cyberbullying assessment instruments: A systematic review. Aggression and violent behavior, 18(2), 320-334.

Bhandari, A., & Bimo, S. (2020). TikTok and the "algorithmized self": A new model of online interaction. AoIR Selected Papers of Internet Research.

Bossler, A. M., & Berenblum, T. (2019). Introduction: new directions in cybercrime research. Journal of Crime and Justice, 42(5), 495-499.

Broadhurst, R., & Chang, L. Y. (2012). Cybercrime in Asia: trends and challenges. Handbook of Asian criminology, 49-63.

Das, S., & Nayak, T. (2013). Impact of cybercrime: Issues and challenges. International journal of engineering sciences & Emerging technologies, 6(2), 142-153.

http://dx.doi.org/10.29009/ijres.7.3.1

Fakhrou, A. A., Adawi, T. R., & Moussa, M. A. (2022). Cybercrime Risk Fear Among University Students' Social Networking Sites: Validity and Reliability. International Journal of Cyber Criminology, 16(1), 40-53.

Gálik, S. (2019). On human identity in cyberspace of digital media. European Journal of Tranformation Studies, 7(2), 33-44.

Gambhir, B. S., Habibkar, J., Sohrot, A., & Dhumal, R. (2022). Cybercrime Detection Using Live Sentiment Analysis. In Pattern Recognition and Data Analysis with Applications (pp. 409-419). Singapore: Springer Nature Singapore.

Giumetti, G. W., & Kowalski, R. M. (2022). Cyberbullying via social media and well-being. Current Opinion in Psychology, 45, 101314.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. Journal in computer virology, 2, 13-20.

Gunitsky, S. (2015). Corrupting the cyber-commons: social media as a tool of autocratic stability. Perspectives on Politics, 13(1), 42-54.

Hazelwood, S. D., & Koon-Magnin, S. (2013). Cyber stalking and cyber harassment legislation in the United States: A qualitative analysis. International Journal of Cyber Criminology, 7(2), 155.

Khandelwal, S., & Chaudhary, A. (2022). COVID-19 pandemic & cyber security issues: Sentiment analysis and topic modeling approach. Journal of Discrete Mathematical Sciences and Cryptography, 25(4), 987-997.

Kirwan, G. (2016). Forensic cyberpsychology. In An Introduction to Cyberpsychology (pp. 161-174). Routledge.

http://dx.doi.org/10.29009/ijres.7.3.1

Kumari, S., Saquib, Z., & Pawar, S. (2018, August). Machine learning approach for text classification in cybercrime. In 2018 Fourth international conference on computing communication control and automation (ICCUBEA) (pp. 1-6). IEEE.

Kurniawan, B. (2018). Tik tok popularism and nationalism: rethinking national identities and boundaries on millennial popular cultures in indonesian context. Proceedings of AICS-Social Sciences, 8, 83-90.

Li, T. B. Q. (2005). Cyber-harassment: A study of a new method for an old behavior. Journal of educational computing research, 32(3), 265-277.

Liu, J., Hebenton, B., & Jou, S. (2012). Progress of Asian criminology: editors' introduction. In Handbook of Asian criminology (pp. 1-7). New York, NY: Springer New York.

Lozano-Blasco, R., Cortés-Pascual, A., & Latorre-Martínez, M. P. (2020). Being a cybervictim and a cyberbully–The duality of cyberbullying: A meta-analysis. Computers in human behavior, 111, 106444.

Mandal, S., Saha, B., & Nag, R. (2020). Exploiting aspect-classified sentiments for cyber-crime analysis and hack prediction. In Trends in Computational Intelligence, Security and Internet of Things: Third International Conference, ICCISIoT 2020, Tripura, India, December 29-30, 2020, Proceedings 3 (pp. 200-212). Springer International Publishing.

http://dx.doi.org/10.29009/ijres.7.3.1

Moussa, M. A. (2020a). Emotional blackmail: theories and patterns (in Arabic). Amman- Jordon: Dar Al-Swaqe Aleimieh.

Moussa, M. A. (2020b). Sentiments analysis in Cyber reality between real and possible (in Arabic). Amman- Jordon: Dar Al-Swaqe Aleimieh.

Ramírez Sánchez, J., Campo-Archbold, A., Zapata Rozo, A., Díaz-López, D., Pastor-Galindo, J., Gómez Mármol, F., & Aponte Díaz, J. (2021). Uncovering cybercrimes in social media through natural language processing. Complexity, 2021, 1-15.

Rosa, H., Pereira, N., Ribeiro, R., Ferreira, P. C., Carvalho, J. P., Oliveira, S., ... & Trancoso, I. (2019). Automatic cyberbullying detection: A systematic review. Computers in Human Behavior, 93, 333-345.

Selkie, E. M., Fales, J. L., & Moreno, M. A. (2016). Cyberbullying prevalence among US middle and high school–aged adolescents: A systematic review and quality assessment. Journal of Adolescent Health, 58(2), 125-133.

Shu, K., Sliva, A., Sampson, J., & Liu, H. (2018). Understanding cyber-attack behaviors with sentimental information on social media. In Social, Cultural, and Behavioral Modeling: 11th International Conference, SBP-BRiMS 2018, Washington, DC, USA, July 10-13, 2018, Proceedings 11 (pp. 377-388). Springer International Publishing.

Sliva, A., Shu, K., & Liu, H. (2019). Using social media to understand cyber-attack behavior. In Advances in Human Factors, Business Management and Society: Proceedings of the AHFE 2018 International Conference on Human Factors, Business

http://dx.doi.org/10.29009/ijres.7.3.1

Management and Society, July 21-25, 2018, Loews Sapphire Falls Resort at Universal Studios, Orlando, Florida, USA 9 (pp. 636-645). Springer International Publishing.

Suler, J. R. (2002). Identity management in cyberspace. Journal of applied psychoanalytic studies, 4, 455-459.

Velasco, C. (2022, May). Cybercrime and Artificial Intelligence. An overview of the work of international organizations on criminal justice and the international applicable instruments. In ERA Forum (Vol. 23, No. 1, pp. 109-126). Berlin/Heidelberg: Springer Berlin Heidelberg.

Whittaker, E., & Kowalski, R. M. (2015). Cyberbullying via social media. Journal of school violence, 14(1), 11-29.

Zuo, H., & Wang, T. (2019). Analysis of Tik Tok user behavior from the perspective of popular culture. Frontiers in Art Research, 1(3).

http://dx.doi.org/10.29009/ijres.7.3.1

ملحق: عبارات مقياس الوعي المدرك للجريمة السيبرانية المرتبطة بمواقع التواصل الاجتماعي

1. قلة القوانين والتشريعات التي تخص وسائل التواصل الاجتماعي.
2. تنمي وسائل التواصل الاجتماعي روح العنف والتعصب لدى المجتمع العماني.
3. تساهم وسائل التواصل الاجتماعي في زيادة النصب الالكتروني بالترويج لبيع بضائع وهمية وغير مرخصة
4. تستغل الجماعات المتطرفة وسائل التوصل الاجتماعي في استقطاب الشباب نحوها والإيمان بأفكارها الهدامة.
5. تُسهم وسائل التوصل الاجتماعي في نشر الشائعات الزائفة.
6. تستغل وسائل التوصل الاجتماعي الأحداث الجارية لنشر الفوضى والفتن في المجتمع العماني.
7. تُحرض وسائل التوصل الاجتماعي على الانتحال الشخصي لصفات وهمية
8. تعد وسائل التوصل الاجتماعي بيئة خصبة للإيقاع بالأفراد والفتيات وتوريطهم في محتويات معينة.
9. تساهم وسائل التواصل الاجتماعي في ارتكاب الجرائم الهجمات السيبرانية بمختلف أنواعها.
10. تنمي وسائل التوصل الاجتماعي دوافع التسلط الالكتروني على الشخصيات بدوافع شخصية مختلفة.

http://dx.doi.org/10.29009/ijres.7.3.1

11. تؤثر وسائل التوصل الاجتماعي على التحقيقات في بعض القضايا العامة.

12. تؤثر وسائل التواصل الاجتماعي على الرأي العام في سلطنة عمان.

13. تساهم وسائل التواصل الاجتماعي في نشر جرائم الابتزاز والاحتيال.

14. تحول وسائل التواصل الاجتماعي القضايا الشخصية إلى قضايا رأي عام كمطاردة الكترونية لبعض الأفراد

15. تؤثر وسائل التواصل الاجتماعي على نتائج الانتخابات في سلطنة عمان.

16. يزداد استخدام تطبيقات الذكاء الاصطناعي على انتاج أصوات ومقاطع فيديو مركبة ويمكنها تركيب محتويات توقع أصحابها في مسائلة قانونية.

http://dx.doi.org/10.29009/ijres.7.3.1