الابتزاز الإلكتروني في المجتمع العماني: إستراتيجيات مقترحة لتفعيل دور المؤسسات التربوية في الحد من الابتزاز للشباب العماني

حفيظة بنت سليمان البراشدية*
سعيد بن سليمان الظفري**

ملخص: تهدف الدراسة الحالية إلى البحث في الابتزاز الإلكتروني في المجتمع العماني من أجل الخروج باستراتيجيات مقترحة لتفعيل دور المؤسسات التعليمية في الحد منه. تبنت الدراسة النهج النوعي حيث أجريت المقابلات الفردية المفتوحة، تلتها جلسات نقاش مركزة، ثم مقابلات جماعية مقننة. تكونت عينة الدراسة من 36 شخصاً منهم 17 من الذطور و 19 من الإناث. بينت النتائج أن طلبة الجامعات والكليات هم الأكثر عرضة للابتزاز، في حين أن ابتزاز الذكور للإناث هو الشكل الأكثر شيوعاً. يعد إرسال طلب صداقة للضحايا من خلال مواقع التوتاصل الاجتماعي أحد الأساليب الأكثر استخداماً من قبل المبتزون الإككترونيون. تمر عملية الابتزاز الإلكتروني عبر المراحل الآتية: الطلب، والمقاومة والضغط والتهديد والطاعة والتكرار. يعتقد 60% من المستجيبين أن وعي الشباب بكيفية التعامل مع حالات الابتزاز الإلكتروني لا يزال غير كاف، في حين يعتقد 80% من المستجيبين أن الجهود المبذولة لزيادة الوعي بالاتزاز الإلكتروني متفرقة وغير منظمة، مما يقلل من فعاليتها ويزيد العواقب طويلة الأجل. يعد الخوف أهم الآثار النفسية للالتزاز الإلكتروني، في حين أن إفساد قيم المجتمع هو أهم الآثار الاجتماعية، بينما توقف الضحية عن الإنتاجية هو أهم الآثار الاقتصادية للابتزاز الإلكتروني. كما تعد حملات التوعية أفضل استراتيجية للحد من الابتزاز الإلكتروني للشباب.

المصطلحات الأساسية: الابتزاز الإلكتروني، المؤسسات التربوية، الشباب العماني.

(*) (**) مجلس البحث العلمي، جامعة السلطان قابوس، سلطنة عمان.
Email: hafidhaalbarashdi@gmail.com

مقدمة:

انتشرت في الآونة الأخيرة ظاهرة الابتزاز الإلكتروني للشباب في دول الخليج العربية، ومنها سلطنة عمان. وغالباً ما يتم الابتزاز الإلكتروني عبر تهديد الضحية وترهيبها بنشر صور أو مواد فيلمية أو تسريب معلومات سرية تخصه، مقابل دفع مبالغ مالية أو استغلال الضحية للقيام بأعمال غير مشروعة، كالإفصاح عن معلومات سرية خاصة بجهة العمل أو غيرها من الأعمال غير القانونية. وعادة ما يتم تصيد الضحايا عن طريق البريد الإلكتروني أو مواقع الشبكات الاجتماعية المختلفة كالفيس بوك، وتويتر، وغيرها؛ وذلك لانتشار استخدامها بين فئة الشباب.

وقد تزايدت عمليات الابتزاز الإلكتروني في ظل تنامي عدد مستخدمي مواقع الشبكات الاجتماعية وبرامج المحادثات المرئية المختلفة بالسلطنة؛ حيث تشير إحصائيات هيئة تقنية المعلومات إلى تسجيل 161 حالة ابتزاز إلكتروني تمت في عام 2016، مقارنة بحالة واحدة فقط في عام 2011. وكانت أغلب حالات الابتزاز بغرض الحصول على المال، أو الحصول على خدمات أخرى من الضحية. وفقاً للإحصاءات السابقة فإن 90% من كل جرائم الابتزاز الإلكتروني تم الإبلاغ عنها من قبل الرجال، بينما الضحايا من الإناث يترددن في الإبلاغ عن هذه الحالات؛ بسبب الخوف من وصمة العار التي تلصق بالضحية. وقد تلقى المركز الوطني للسلامة المعلوماتية التابع لهيئة تقنية المعلومات خلال الحملة التوعوية الأولى حول الابتزاز الإلكتروني (بلغ وسرك في بير) التي تمت خلال الفترة من 4 إلى 18 أكتوبر 2016 أكثر من 2800 اتصال هاتفي وأكثر من 420 بريداً إلكترونياً للتبليغ عن حالات الابتزاز الإلكتروني، وبعد تحليل تلك المكالمات والرسائل سجلت أكثر من 163 حالة ابتزاز، وبذلك يصل إجمالي حالات الابتزاز الإلكتروني المسجلة في المركز إلى 324 حالة، كما ارتفعت نسبة الإناث اللاتي يبلغن عن حالة الابتزاز الإلكتروني من 10% إلى 38% بعد الحملة؛ مما يؤكد وجود حاجة ماسة للتوعية حول الابتزاز الإلكتروني (هيئة تقنية المعلومات، 2017؛ الوطن، 2016).

ويعرف حميد (2011) الابتزاز – كمصطلح – بأنه "محاولة تحصيل مكاسب مادية أو معنوية من شخص أو أشخاص طبيعيين أو اعتباريين بالإكراه عن طريق التهديد بفضح سر من وقع عليه الابتزاز، أو استغلال القوة مقابل ضعف إنسان آخر سواء كان هذا الضعف مؤقتاً أم دائماً، ومحاولة للإكراه وسلب الإرادة والحرية لإيقاع

الأذى الجسدي أو المعنوي على الضحايا عن طريق وسائل يتفنن الجاني في استخدامها لتحقيق جرائمه الأخلاقية أو المادية أو كليهما معاً" (حميد، 2011: 14).

وهناك عدة أنواع من الابتزاز، منها: الابتزاز المادي؛ ويتم عبر علاقة هشة بين شخصين متخاصمين، يسودها التأثير القوي للمال على النفوس، إلى حد يجعل الصديق يبيع صديقه أو قريبه وربما أخاه من أجل الحصول على المال، وهناك الابتزاز الإلكتروني، الذي ظهر بعد تعدد وسائل الاتصال الحديثة من الإنترنت وتنوعها، والهواتف الذكية ووسائل التواصل الاجتماعي، وهو استخدام تقنية المعلومات والاتصالات أداة لإجبار أو إكراه أو تهديد شخص أو مؤسسة أو جماعة بكشف سر من أسرارهم ما لم يحصل المبتز على مكاسب مادية أو معنوية، وهناك الابتزاز الأخلاقي الجنسي؛ حيث يقوم المبتز بطلب أشياء جنسية من الضحية، أما أخطر أنواع الابتزاز فهو الابتزاز العاطفي؛ حيث يُستخدم لتحقيق سيطرة عاطفية ونفسية على الضحية من خلال جعله يشعر بأنه مدين أو مذنب في حق الشخص الذي يبتزه؛ فينفذ له طلباته، وهذا النوع من الابتزاز لا يجرمه القانون (الفالح، 2011). كما يتخذ الابتزاز أشكالاً مختلفة ومتعددة، منها: ابتزاز الفتيات للشباب، أو ابتزاز الشباب للفتيات، أو ابتزاز الفتيات للفتيات، أو ابتزاز الشباب للشباب (الحمين، 2011).

وهناك كثير من العواقب المترتبة على هذه الجريمة، سواء على الفرد أو المجتمع، ومن أهمها أن هذه الجريمة تؤدي إلى جرائم أخرى في المجتمع، من مثل: الزنى، والقتل، والدعارة، والانتحار، فضلاً عن انتشار الفوضى والخوف وعدم الطمأنينة، وانتشار الأمراض النفسية والجنسية، أما العواقب النفسية التي قد تصيب الضحية فتتمثل في الترهيب النفسي، والقلق والتوتر، والشعور الدائم بالذنب، والأرق والسهر وصعوبات النوم، وتكرار الكوابيس الليلية، وعدم التركيز، والخوف، وترك العمل أحياناً على الرغم من الحاجة إلى المال، والعصبية التي تنعكس على العمل والبيت، وقلة الإنتاج في العمل، كما قد تؤدي هذه الحالة أحياناً إلى الانهيار العصبي (البداينة، 2014؛ الحمين، 2011).

لذا أولت حكومة السلطنة اهتماماً كبيراً لمكافحة الابتزاز الإلكتروني؛ نظراً للعواقب الوخيمة المترتبة عليه سواء على الأفراد أو المجتمع ككل؛ ومن ثم أصدرت قانوناً لمكافحة جرائم تقنية المعلومات، ينص في مادته الثامنة عشرة على أنه: "يعاقب بالسجن مدة لا تقل عن شهر ولا تزيد على ثلاث سنوات وبغرامة لا تقل

عن ألف ريال عماني ولا تزيد على ثلاثة آلاف ريال عماني أو بإحدى هاتين العقوبتين، كل من استخدم الشبكة المعلوماتية أو وسائل تقنية المعلومات في تهديد شخص أو ابتزازه لحمله على القيام بفعل أو امتناع ولو كان هذا الفعل أو الامتناع عنه مشروعاً، وتكون العقوبة السجن المؤقت مدة لا تقل عن ثلاث سنوات ولا تزيد على عشر سنوات وغرامة لا تقل عن ثلاثة آلاف ريال عماني ولا تزيد على عشرة آلاف ريال عماني إذا كان التهديد بارتكاب جناية أو بإسناد أمور مخلة بالشرف أو الاعتبار" (المركز الوطني للسلامة المعلوماتية، 2017).

ويمكن الوقاية من وقوع جرائم الابتزاز الإلكتروني من خلال قيام الجهات المختصة بتوعية الشباب في المدارس والكليات حول مفهوم الابتزاز الإلكتروني وطرقه ووسائله، وكيفية تجنبه والتعامل مع المبتزين. كما يمكن تجنب وقوع جريمة الابتزاز الإلكتروني من خلال توعيه الوالدين، وحثهما على تحذير أبنائهما من إفشاء أسرارهم وبياناتهم الشخصية عبر شبكة الإنترنت، وتثقيفهم دينياً ورقمياً، ومراقبة سلوكياتهم، وعدم إعطائهم الحرية الكاملة في استخدام وسائل الاتصال، ومواقع الشبكات الاجتماعية.

وفيما يلي سنعرض للدراسات السابقة التي سلطت الضوء على آثار الابتزاز، ومنها دراسة جوميزا وجانوزا (Gómeza & Ganuza, 2002) التي بينت الفروق بين ثلاثة أنظمة قانونية بديلة، هي: الابتزاز من خلال عقد قابل للنفاذ قانونياً، والابتزاز من خلال عقد باطل، والابتزاز الجنائي. وحاولت الدراسة استكشاف مبررات تجريم الابتزاز، بما ينسجم مع قانون الابتزاز. وقد بينت نتائج الدراسة أن أسباب تجريم الابتزاز هو أثره في زعزعة الاستقرار الاجتماعي، في كونه قائماً على تفاعل من طرف أقوى لطرف أقل قوة، وبسبب نتائج الابتزاز المضرة بالأفراد والمجتمع، وتفسر هذه النتيجة سبب التزام معظم النظم القانونية بتجريم الابتزاز.

وحول الآثار النفسية للابتزاز، قامت دراسة ليوا (Liua, 2010) باستكشاف العلاقة بين تصور الموظفين للابتزاز العاطفي في بيئة العمل في تايوان. كما حاولت الدراسة تقديم فهم أفضل لمفهوم الابتزاز العاطفي وتأثيراته النفسية. وقد جمعت البيانات من خلال استبانات وزعت على عينة مكونة من 299 موظفاً. ووجدت الدراسة أن الابتزاز العاطفي يرتبط ارتباطاً سلبياً بالرفاهية؛ إذ إن الشركات التي

تجعل الموظفين يشعرون بابتزاز عاطفي قوي، تنخفض معنوياتهم وينعكس ذلك سلباً على حالتهم النفسية.

ومن الدراسات التي تناولت دوافع الابتزاز الإلكتروني دراسة ميشيل (Miceli, 2011)، التي بينت أن الحصول على معلومات سرية عن الضحية يؤدي إلى استغلاله مادياً. وقد ناقشت الدراسة أهمية المعلومات وخطورتها. وأظهرت أنه، في حين أن للمعلومات قيمة اقتصادية؛ بمعنى أن تسهم في تحسين كفاءة السوق، فإن لها قيمة خاصة إذا ما وجدت عند طرف ثالث لا يلتزم بمعايير القيم الاجتماعية. في حالة الابتزاز يتم استخدام المعلومات بهدف الاستحواذ والإخفاء؛ وذلك للحصول على المال أو المزيد من المعلومات أو الخدمات بشكل غير قانوني .

ومن الدراسات التي تطرقت للأساليب التقنية المستخدمة في جرائم الابتزاز دراسة آل النمر، والشهري، وآل سليمان، والغامدي (2013)، وكانت عن دور تقنية المعلومات في مكافحة جرائم الابتزاز. تشكل مجتمع الدراسة من العاملين في مجال تقنية المعلومات وعددهم الإجمالي 164 فرداً، بينما بلغ حجم العينة 115 فرداً. استخدمت الدراسة المنهج الوصفي التحليلي والاستبانة أداة لجمع البيانات. بينت النتائج أن أهم أدوار تقنية المعلومات في مكافحة جرائم الابتزاز يكون من خلال: تحديد موقع مرتكب جريمة الابتزاز، والتقاط الدليل الإلكتروني لإثبات جريمة الابتزاز، وتسجيل المحادثات التي تتضمن تهديدات المبتز للضحية. كما بينت النتائج أن الإجراءات التي تشير إلى فاعلية تقنية المعلومات في مكافحة جرائم الابتزاز هي: سرعة التقاط الدليل الإلكتروني اللازم لإثبات جريمة الابتزاز، والدقة في تحديد موقع مرتكب جريمة الابتزاز، والدقة في تحديد تاريخ ارتكاب جريمة الابتزاز، وأن وسائل تقنية المعلومات المستخدمة في إثبات جرائم الابتزاز هي: استخدام عناوين (IP) لتحديد موقع مرتكب جريمة الابتزاز، واستخدام عناوين (IP) لتحديد تاريخ ارتكاب جريمة الابتزاز، واستخدام البروكسي في التقاط الدليل الإلكتروني اللازم لإثبات جريمة الابتزاز. وتشير النتائج إلى أن المعوقات المهمة التي تحد من فاعلية تقنية المعلومات في مكافحة جرائم الابتزاز بدرجة مرتفعة هي: قلة تزويد الجهات المعنية بمكافحة الابتزاز بتقنية المعلومات اللازمة لمكافحة الابتزاز، وقلة الكوادر البشرية المؤهلة لاستخدام تقنية المعلومات في مكافحة الابتزاز، وندرة الإمكانات الفنية اللازمة لتشغيل وصيانة تقنية المعلومات اللازمة

لمكافحة الابتزاز. أما أهم الوسائل للتغلب على المعوقات التي تحد من فاعلية تقنية المعلومات في مكافحة جرائم الابتزاز فهي: تزويد الجهات المعنية بمكافحة الابتزاز بتقنية المعلومات اللازمة لمكافحة الابتزاز، وتدريب الكوادر البشرية اللازمة لاستخدام تقنية المعلومات في مكافحة الابتزاز، والتزام السرية التامة نحو من تعرضوا للابتزاز من الأفراد أو الشركات. وأخيراً بينت النتائج أن أفراد عينة الدراسة لديهم رؤية متشابهة نحو وسائل التغلب على المعوقات التي تحد من فاعلية تقنية المعلومات في مكافحة جرائم الابتزاز مهما اختلفت مؤهلاتهم التعليمية.

وقام رامدينماوي، وآخرون (Ramdinmawii, et al., 2014) بدراسة وصفية تناولت عدة محاور، هي: الطرق والوسائل المستخدمة في الجرائم السيبرانية، وجرائم الابتزاز الإلكتروني، والأنواع الشائعة من الجرائم السيبرانية، والمناطق التي تكثر فيها تلك الجرائم، والعواقب الاقتصادية للجرائم السيبرانية، وما تسببه من خسائر مالية هائلة في العديد من البلدان، وخاصة في مجالات المبيعات والاستثمارات، والغرامات والعقوبات المختلفة، التي وضعتها الدول لهذه الفئة من الجرائم، وقد ركزت الدراسة على الجرائم السيبرانية المتصلة بالرسائل الإلكترونية. كما عرضت الدراسة بعض حالات جرائم الابتزاز الإلكتروني.

ومن الدراسات التي تطرقت لأسباب وقوع الضحايا في عمليات الابتزاز دراسة أجراها المركز الوطني للإحصاء والمعلومات العماني بالتعاون مع مجلس البحث العلمي (2015) حول قيم الشباب العماني، تضمنت استخدام الشباب لوسائل التواصل الاجتماعي وثقتهم في تلك الوسائل. طبقت على عينة مكونة من 1243مواطناً عمانياً في فئة الشباب 18–29 سنة، شملت جميع محافظات السلطنة، ومختلف المستويات التعليمية والفئات العمرية والذكور والإناث. وقد تباينت آراء الشباب حول ما يمكن أن ينشروه أو يشاركوا به على صفحات التواصل الاجتماعي بشكل آمن، فبينما يرى ثلثا الشباب 63% أن تلك المواقع آمنة جدًا أو آمنة إلى حد ما لعرض الآراء الخاصة والمشاركة في وجهات النظر، نجد أن تلك النسبة تنخفض بدرجة كبيرة عندما يتعلق الأمر بمشاركة البيانات الشخصية أو الصور والفيديوهات الخاصة والعائلية؛ حيث تصل إلى 29% فقط. وأظهرت النتائج وجود بعض التفاوت في مدى الاعتقاد بأن مواقع التواصل الاجتماعي تعد مكاناً آمناً لعرض الآخرين ومشاركتهم الآراء الخاصة والبيانات والصور والفيديوهات الشخصية. وبشكل عام، يزيد الاعتقاد بالأمان حول مشاركة الآخرين البيانات

الشخصية لدى الذكور عن الإناث، وكانت النسبة 35% للذكور مقابل 22% للإناث. أما الصور والفيديوهات الشخصية فكانت 25% للذكور مقابل 16% للإناث، وفي المقابل يزيد الاعتقاد بالأمان فيما يتعلق بمشاركة الآراء الخاصة ووجهات النظر لدى الإناث 70% عن الذكور 58%و، مع ارتفاع مستوى التعليم يزداد الشعور بالأمان عند مشاركة الآخرين الآراء الخاصة ووجهات النظر إلى 66% للحاصلين على تعليم أعلى من الثانوي مقابل 55% للحاصلين على تعليم أقل من الثانوي، ويقل الاعتقاد بالأمان عند مشاركة الصور والفيديوهات الشخصية والعائلية، بينما لا تختلف النسب فيما يتعلق بمشاركة البيانات الشخصية. وبشكل عام، تقل نسبة الاعتقاد بالأمان عند استخدام مواقع التواصل الاجتماعي مع تقدم العمر وخصوصاً فيما يتعلق بنشر البيانات الشخصية ومشاركتها بنسبة 21%.

وفي المملكة المتحدة أجرى وولاك وفينكلهور (Wolak & Finkelhor, 2016) مسحاً إلكترونياً استهدف 1631 من ضحايا الابتزاز الجنسي الإلكتروني المهددين بفضح صور جنسية لهم عبر الفيسبوك، كان معظم الضحايا من الإناث بنسبة 83% و40% منهن في العشرينيات من العمر. بينت نتائج الدراسة أن أسباب الابتزاز الجنسي الإلكتروني كانت متنوعة، ولكن حوادث الابتزاز قد وقعت على نطاق واسع عبر طريقتين: إما في أعقاب لقاء وجهاً لوجه مع الضحية في علاقة رومانسية أو جنسية تم فيها أخذ الصور الجنسية، أو استخدم الجاني صورة جنسية تم الحصول عليها من الضحية الذي التقى به عبر الإنترنت. وقد بينت نتائج الدراسة أن مرتكبي التهديدات قاموا بإيذاء الضحية جسدياً في نحو 45% من حالات الابتزاز، بينما استمرت التهديدات لمدة 6 أشهر أو أكثر. وتم نشر الصور الجنسية للضحية في نحو 30% من الحالات. كما بينت النتائج أن واحداً من بين كل خمسة ضحايا حاولوا الحصول على مساعدة والإبلاغ عن حالة الابتزاز عبر موقع ويب أو تطبيق خاص بالابتزاز، بينما 16% من المستجيبين لجؤوا للشرطة. وقد أوصت الدراسة بضرورة اتخاذ إجراءات استباقية للوقاية من الابتزاز عبر المناهج الدراسية.

ومن الدراسات التي اهتمت بمعرفة الفئات العمرية المعرضة للابتزاز ومدى انتشار الابتزاز في المجتمع، دراسة الغامدي وعبده (2016)، التي هدفت إلى تحديد مدى انتشار مشكلة الابتزاز الجنسي لدى الشباب من طلاب جامعة الباحة، واستخدمت الدراسة عينة مكونة من 1859 طالباً وطالبة، منهم 48,1% من الإناث، و51,3% من الذكور. طبقت الدراسة اختبار الابتزاز الجنسي، ويتكون من صورتين:

صورة خاصة بالذكور وأخرى خاصة بالإناث. ويتكون الاختبار من 56 عبارة، تقيس سبعة أبعاد يتضمنها سلوك الابتزاز وهي العدوان، والقلق النفسي، والاكتئاب النفسي، وفعل الابتزاز، والآثار الناتجة منه، وأساليب التربية، وأساليب التربية الإسلامية. وقيس معامل ثبات للاختبار فكان 0,80. كشفت نتائج الدراسة انتشار مشكلة الابتزاز الجنسي بين الشباب الذكور بصورة دالة إحصائياً، وبينت النتائج فروقاً دالة بين الذكور والإناث في ممارسة الابتزاز الجنسي لصالح الذكور؛ فهم أكثر ممارسة لسلوك الابتزاز والعدوان من الإناث. وقد أوصت الدراسة بتنفيذ برامج توعوية وإرشادية حول الابتزاز الإلكتروني وطرق تجنبه ومخاطره الاجتماعية.

وقدم كوبسكي (Kopecky, 2017) دراسة عن ابتزاز الأطفال في التشيك. هدفت إلى تعرف إذا ما كانت هناك فروق في الجنس والعمر ترتبط بظاهرة الابتزاز، وكذلك حاولت الدراسة استكشاف مدى إمكانية تحول الأطفال المشاركين في الابتزاز إلى مرتكبين لهذه الجرائم. تم جمع البيانات من خلال البحوث التي أجراها مركز منع الاتصالات الظاهرية الخطرة بكلية التربية في جامعة بالاكي في الفترة (2013–2015). كما أجريت دراسة حالة مفصلة عن 25 حالة خطيرة من الابتزاز على الإنترنت. وقد توصلت الدراسة إلى نموذج مكون من مراحل متصلة يتم من خلالها تنفيذ الهجوم عبر الإنترنت استناداً إلى تحليل الحالات الفردية، ويمكن للنموذج التنبؤ بالاتصالات من المهاجم إلى الضحية. وقد أوصت الدراسة بتوعية الآباء والأمهات حول التقنيات التي يستخدمها مبتزو الأطفال؛ حيث تركز هذه التقنيات على اكتساب ثقة الطفل، ثم الإغراء بالمواد الحميمة والحصول على انتباه الطفل، ثم يبدأ الجاني في تقييم كل المواد المرسلة من قبل الضحية للقيام بعملية ابتزاز فعالة. وللأسف فإن 100% من الأطفال الضحايا لم يطلبوا مساعدة شخص بالغ خلال 2–3 أشهر من الابتزاز.

وتتميز الدراسة الحالية عن الدراسات السابقة من حيث كونها بحثت في التفاصيل الدقيقة المتعلقة بأشكال الابتزاز وأسبابه وأساليبه؛ وذلك بهدف طرح إستراتيجيات ملائمة لتفعيل دور المؤسسات التربوية في الحد من ظاهرة الابتزاز الإلكتروني للشباب العماني لتكون بمثابة دليل إرشادي للوقاية من التعرض لجرائم المعلوماتية؛ وذلك بناء على المعلومات التي سيتم جمعها من خلال الدراسة. ركزت الدراسة أيضاً على دور المؤسسات التربوية في نشر التوعية حول الابتزاز؛ نظراً لأهمية إكساب طلبة المدارس هذه الوقاية قبل انطلاقهم لمؤسسات التعليم العالي وجهات العمل؛ حيث تزيد هناك

فرص تعرضهم للوقوع في الابتزاز. كما تختلف الدراسة الحالية من حيث كونها قارنت بين آراء خبراء أمن المعلومات وآراء الاختصاصيين الاجتماعيين والنفسيين في المدارس حول أشكال الابتزاز وأساليبه وإستراتيجيات الوقاية منه لاستكشاف مدى وعي الاختصاصيين في المدراس وإلمامهم بالطرق الحديثة والمتعددة للابتزاز، فضلاً عن استكشاف مدى إدراكهم لخطورة المشكلة وتزايد حجمها؛ حيث يمتلك الاختصاصيون المعرفة بكيفية التعامل نفسياً واجتماعياً مع الحالات بعد وقوعها، ولكنهم يفتقرون إلى المعرفة التقنية لكيفية حدوثها، وهو أمر مهم في مجال التوعية، وبالمقابل يمتلك الخبراء المعرفة التقنية ولكنهم لا يملكون القدر الكافي من المعرفة النفسية بكيفية التعامل مع الضحايا.

مشكلة الدراسة:

لقد صاحب التطور التكنولوجي الهائل انتشار واسع للأجهزة الإلكترونية المختلفة، من مثل: أجهزة التصوير، وأجهزة الاتصالات بكافة أشكالها وأنواعها، ومواقع الشبكات الاجتماعية المختلفة. كما صاحب ذلك الرغبة الشديدة من جميع أفراد المجتمع بمختلف طبقاته في اقتنائها، والاستفادة منها، ولاسيما الشباب والفتيات الذين انبهروا بهذه التقنيات والوسائل، واستخدموها بكل ما فيها من إيجابيات وسلبيات، دون مراعاة للضوابط الشرعية في استخدامها؛ فتجاوزوا الشرع بالدخول إلى غرف المحادثات بين الجنسين سواء الصوتية، أو المرئية، وتساهل الشباب والشابات في تصوير أنفسهم، وغيرهم، وتبادل هذه الصور فيما بينهم، وإرسالها عبر هذه التقنيات المختلفة، مما جعلهم فريسة سهلة لجرائم الابتزاز الإلكتروني (المطلق، 2016).

كما أن الابتزاز الإلكتروني يتم أيضاً من خلال عصابات متخصصة متعددة الجنسيات، تقوم بتسجيل مقاطع فيديو غير لائقة للضحايا عبر الإنترنت، ثم تهددهم بنشرها ما لم يدفعوا مبالغ مالية ضخمة؛ حيث تجذب هذه العصابات الشباب عبر محادثة سريعة مع من يعتقدون أنه فتاة، ثم تتطور إلى محادثات ساخنة وممارسات إباحية، ثم تبدأ عملية الابتزاز، التي قد تمتد لفترة طويلة لتحقيق مصالح مادية. وللأسف فإن بعض الشباب الباحث عن الحب أو الجنس أصبح هدفاً ثميناً لتلك العصابات، التي تبتكر العديد من الطرق والأساليب للإيقاع بهم، وتوريطهم، ثم ابتزازهم بطرق مبتذلة؛ بهدف الحصول على المال مقابل عدم التشهير بهم.

ولفهم سيكولوجية الابتزاز ميز الصالح (2011) بين شخصيتي الجاني والمجني عليه في جرائم الابتزاز الإلكتروني؛ حيث يتسم الجاني(المبتز) بالشخصية السيكوباتية، وهي شخصية معتلة نفسياً تتسم بعدم النضج الانفعالي، واختلال الخلق، والرغبة في خرق القانون الخُلقي السائد في المجتمع، ومن أهم صفاته الاندفاع والتهور، والسلوك المضاد للمجتمع، الذي لا يراعي قيمه وأعرافه، ويغيب عنده الضمير والخجل، والعجز عن تكوين علاقة حب ومودة واقعية مع غيره من الناس، كما يتسم بالقسوة مع عدم الشعور بالإثم. أما المجني عليه (الضحية أو المُبتز)؛ فهو عادة شخص يعاني من اضطراب سلوكي، وعدم استقرار عائلي؛ مما يدفعه إلى اللجوء إلى ممارسات سرية تعوضه عن غياب الأسرة. كما يعاني نوعاً من انعدام الثقة بالنفس، وسهولة التأثير عليه؛ الأمر الذي يجعله صيداً سهلاً للمبتزين. وغالباً ما يكون شخصاً عاش، أو جرب، أو واجه حدثاً، أو أحداثاً، نتج عنها الموت، أو تهديد بالموت، أو جروح خطيرة، أو تهديد كيانه الجسدي؛ مما جعله يحس بالخوف والذعر، وعدم وجود من يقدم له العون والمساعدة، وبالطبع تكون الفئات العمرية الأصغر عمراً أقل قدرة على التصرف الصحيح في حالة التعرض للابتزاز؛ لذا وجب على المؤسسات التربوية تقديم جرعات كافية من التوعية المستمرة.

وتكمن المشكلة في ضرورة فهم ظاهرة الابتزاز فهماً دقيقاً من حيث دوافع المبتز وأسباب رضوخ الضحية والانجراف معه فيما لا تحمد عقباه على الرغم من أن حل مشكلة الابتزاز يكون بسيطاً جداً؛ فعلى الرغم من أهمية وخطورة الأدلة التي قد يمتلكها المبتز – بحسب اعتقاد الضحية – فما على الضحية سوى التواصل مع الأجهزة الأمنية والإبلاغ عن الجاني وتزويدهم بالأدلة ضده لتنتهي بذلك مشكلته في منتهى السرية. ولكن نظراً لعدم وعي الشباب بطرق السلامة المعلوماتية وأساليبها، وكيفية التعامل مع مواقف الابتزاز نجدهم يشعرون بالخوف والضعف ويميلون للتكتم على الأمر؛ مما يجعلهم يرضخون لتهديدات المبتز. لذا فإن تفعيل دور المؤسسات التربوية في الحد من ظاهرة الابتزاز الإلكتروني من خلال إستراتيجية منهجية تقوم على بث التوعية المستمرة سيكون له أكبر الأثر في الحد من انتشار الظاهرة؛ وذلك نظراً لأن التأسيس الصحيح لطلبة المدارس والجامعات والكليات حسن التعامل مع التكنولوجيا، وتجنب الجرائم المرتبطة بها سيكون الخطوة الوقائية التي ستقلل هذه الظاهرة في المجتمع وتحد منها مستقبلاً.

وفي ظل قلة الدراسات التي أجريت عن الابتزاز الإلكتروني في سلطنة عمان، فإن الدراسة الحالية التي تعد الأولى من نوعها في السلطنة – على حد علم الباحثين– تسعى إلى تسليط الضوء على هذه الظاهرة ودراستها من جميع النواحي، وذلك لأجل وضع إستراتيجية مقننة لتفعيل دور المؤسسات التربوية في توعية الشباب حول الابتزاز الإلكتروني، ومن ثم الحد من انتشار هذه الظاهرة.

أسئلة الدراسة:

تسعى الدراسة الحالية للإجابة عن الأسئلة الآتية:

1 – هل توجد فروق دالة إحصائياً بين الخبراء المتطوعين للتوعية بجرائم الابتزاز الإلكتروني والاختصاصيين الاجتماعيين والنفسيين في تقديرهم لحجم انتشار ظاهرة الابتزاز الإلكتروني في المجتمع العماني؟

2 – هل توجد فروق دالة إحصائياً بين الخبراء المتطوعين للتوعية بجرائم الابتزاز الإلكتروني والاختصاصيين الاجتماعيين والنفسيين في تقديرهم أي فئات المجتمع هي الأكثر عرضة لجرائم الابتزاز الإلكتروني؟

3 – ما أبرز أشكال الابتزاز الإلكتروني التي يتعرض لها ضحايا جرائم الابتزاز الإلكتروني في السلطنة من وجهة نظر المبحوثين؟

4 – ما أهم الأساليب التقنية المستخدمة في الابتزاز الإلكتروني من وجهة نظر المبحوثين؟

5 – كيف تتطور حالات الابتزاز الإلكتروني؟ وما المراحل التي تمر بها من وجهة نظر المبحوثين؟

6 – ما مدى وعي الشباب العماني بكيفية التعامل مع مواقف الابتزاز الإلكتروني من وجهة نظر المبحوثين؟

7 – ما مدى كفاية الجهود الحكومية والتطوعية في توعية الشباب العماني بجرائم الابتزاز الإلكتروني من وجهة نظر المبحوثين؟

8 – ما الآثار النفسية والاجتماعية المترتبة على الوقوع ضحية الابتزاز الإلكتروني من وجهة نظر المبحوثين؟

9 – ما الإستراتيجيات الممكنة لتفعيل دور المؤسسات التربوية في الحد من ظاهرة الابتزاز الإلكتروني للشباب العماني من وجهة نظر المبحوثين؟

أهداف الدراسة:

تهدف هذه الدراسة إلى:

1 – الكشف عما إذا كان هناك فروق دالة إحصائياً بين الخبراء المتطوعين للتوعية بجرائم الابتزاز الإلكتروني والاختصاصيين الاجتماعيين والنفسيين في تقديرهم لحجم انتشار ظاهرة الابتزاز الإلكتروني في المجتمع العماني.

2 – استقصاء مدى وجود فروق دالة إحصائياً بين الخبراء المتطوعين للتوعية بجرائم الابتزاز الإلكتروني والاختصاصيين الاجتماعيين والنفسيين في تقديرهم أي فئات المجتمع هي الأكثر عرضة لجرائم الابتزاز الإلكتروني.

3 – تعرف أبرز أشكال الابتزاز الإلكتروني التي يتعرض لها ضحايا جرائم الابتزاز الإلكتروني في السلطنة من وجهة نظر المبحوثين.

4 – تحديد أهم الأساليب التقنية المستخدمة في الابتزاز الإلكتروني من وجهة نظر المبحوثين.

5 – توضيح كيفية تطور حالات الابتزاز الإلكتروني والمراحل التي تمر بها من وجهة نظر المبحوثين.

6 – تعرف مدى وعي الشباب العماني بكيفية التعامل مع مواقف الابتزاز الإلكتروني من وجهة نظر المبحوثين.

7 – تقييم مدى كفاية الجهود الحكومية والتطوعية في توعية الشباب العماني بجرائم الابتزاز الإلكتروني من وجهة نظر المبحوثين.

8 – الكشف عن الآثار النفسية والاجتماعية المترتبة على الوقوع ضحية الابتزاز الإلكتروني من وجهة نظر المبحوثين.

9 – اقتراح بعض الإستراتيجيات لتفعيل دور المؤسسات التربوية في الحد من ظاهرة الابتزاز الإلكتروني للشباب العماني من وجهة نظر المبحوثين.

المصطلحات الإجرائية للدراسة:

– الابتزاز الإلكتروني: يعرف حميد (2011: 14) الابتزاز بأنه "محاولة تحصيل مكاسب مادية أو معنوية من شخص أو أشخاص طبيعيين أو اعتباريين بالإكراه بالتهديد بفضح سر من وقع عليه الابتزاز، أو استغلال القوة مقابل ضعف إنسان آخر سواء كان هذا الضعف مؤقتاً أم دائماً، ومحاولة للإكراه وسلب الإرادة والحرية

لإيقاع الأذى الجسدي أو المعنوي على الضحايا عن طريق وسائل يتفنن الجاني في استخدامها لتحقيق جرائمه الأخلاقية أو المادية أو كليهما معاً"، بينما تعرف الدراسة الحالية الابتزاز الإلكتروني بأنه: "استخدام تقنية المعلومات والاتصالات كأداة لإجبار شخص أو مؤسسة أو جماعة أو إكراههم أو تهديدهم بكشف سر من أسرارهم ما لم يحصل المبتز على مكاسب مادية أو معنوية.

– **المؤسسات التربوية:** هي جميع المؤسسات التعليمية والتربوية في السلطنة كالمدارس والجامعات والكليات الحكومية والخاصة.

– **الشباب العماني:** هم السكان العمانيون في الفئة العمرية من (15–29) سنة، بحسب تعريف منظمة الأمم المتحدة للتربية والعلوم والثقافة (unesco.org, 2018).

حدود الدراسة:

– حدود موضوعية: اقتصرت هذه الدراسة على ظاهرة الابتزاز الإلكتروني في المجتمع العماني.

– حدود زمانية: اقتصر تطبيق الدراسة الحالية على الفترة من أبريل 2017 إلى أبريل 2018.

– حدود بشرية: اقتصر تطبيق الدراسة الحالية على عينات الدراسة من الخبراء المتطوعين للتوعية بجرائم الابتزاز الإلكتروني والاختصاصيين الاجتماعيين والنفسيين.

أهمية الدراسة:

– الأهمية النظرية: تظهر أهمية هذه الدراسة من خلال إسهامها في إثراء الأدبيات السوسيولوجية حول ظاهرة الابتزاز الإلكتروني التي ازدادت في الآونة الأخيرة بشكل واضح، واتسع نطاق تأثيراتها النفسية والاجتماعية على الأفراد والمجتمعات؛ الأمر الذي يدعو إلى دراسة وتسليط الضوء على هذه الظاهرة في مجتمعنا العماني، ومن المأمول أن تكون هذه الدراسة تمهيداً لإجراء المزيد من الدراسات المماثلة؛ مما سيسهم في تحقيق التراكم المعرفي والبحثي، وهناك أهمية نظرية أخرى تتمثل في محاولة ارتياد حقل بحثي جديد في مجال الإعلام ووسائل الاتصال قائم على دراسة الجرائم الإلكترونية.

– الأهمية التطبيقية: نظراً لانتشار ظاهرة الابتزاز الإلكتروني في المجتمع

العماني، فإن هذا البحث يهدف إلى جمع معلومات كافية عن ظاهرة الابتزاز الإلكتروني في المجتمع العماني؛ وذلك لأجل وضع إستراتيجية مقترحة لتفعيل دور المؤسسات التربوية في الحد من ظاهرة الابتزاز الإلكتروني.

المنهجية والإجراءات:

اعتمدت الدراسة الحالية المنهج الوصفي التطبيقي؛ حيث أجريت مقابلات فردية، ثم مقابلات جماعية مع مجموعتين، الأولى من المختصين في مجال مكافحة الجرائم الإلكترونية وجرائم الابتزاز، والثانية مجموعة من الاختصاصيين الاجتماعيين والنفسيين بوزارة التربية والتعليم، وقد أجريت المقابلات على مرحلتين وبشكل منفصل، اتبعت كل منها جلسات نقاش مركزة (بؤرية) حول قصص الابتزاز الإلكتروني وحالاته في السلطنة، وبعد ذلك تم إجراء تحليل هذه البيانات باستخدام برنامج الأطلس. تي أي 8.

مجتمع الدراسة وعينتها:

تكون مجتمع الدراسة من جميع خبراء أمن المعلومات المتطوعين لمكافحة جرائم المعلومات ضمن سفراء مركز السلامة المعلوماتية العماني، البالغ عددهم (185) خبيراً وخبيرة، وكذلك جميع الاختصاصيين الاجتماعيين والنفسيين العاملين في محافظة مسقط، البالغ عددهم (157) اختصاصياً واختصاصية، وقد تم اختيار هاتين الفئتين؛ نظراً لامتلاكهما الإجابات الدقيقة حول أسئلة الدراسة؛ وذلك نظراً لتعاملهما اليومي مع حالات الابتزاز الإلكتروني وقصصه في المجتمعين المدرسي والمحلي.

أما عينة الدراسة فقد تألفت من 36 شخصاً، منهم 17 من الذكور، 19 من الإناث، قسموا إلى مجموعتين: مجموعة خبراء أمن المعلومات، وهم متطوعون للتوعية بالابتزاز الإلكتروني وعددهم 20 خبيراً وخبيرة، ومجموعة الاختصاصيين الاجتماعيين والنفسيين، وعددهم 16 اختصاصياً واختصاصية. بالنسبة للخبراء، فقد تمت دعوتهم للمشاركة الطوعية في الدراسة من خلال رابط أرسل لمجموعة الواتساب المشاركين فيها بإشراف مركز السلامة المعلوماتية. وقد سجل 30 مشاركاً عبر الرابط، ثم تم التواصل معهم هاتفياً وتحديد موعد المشاركة. وقد تمكن 20 مشاركاً فقط من الحضور. أما الاختصاصيون الاجتماعيون والنفسيون، فقد تم

التواصل مع وزارة التربية والتعليم لترشيح 20 مشاركاً، وبعد تسلم كشف المرشحين تم التواصل معهم هاتفياً لتحديد موعد المشاركة ومكانها. وقد حضر منهم 16 اختصاصياً واختصاصية فقط. وقد تم اختيار حجم العينة؛ بحيث يكون ملائماً لتطبيق المقابلات الجماعية وإجراء حلقات النقاش البؤرية وليكون النقاش والتفاعل بين المشاركين ميسراً، وفي الوقت نفسه يمكن ضبط النقاش والخروج بأفكار شاملة وجوهرية حول موضوع الدراسة، وفيما يلي التفاصيل المتعلقة بعينات الدراسة وكيفية توزيع المشاركين فيها:

أولاً – عينة المقابلات الفردية المفتوحة: تم تطبيقها على عدد من الخبراء في مجال أمن المعلومات من المتطوعين لمكافحة جرائم الابتزاز والتوعية بشأنها، يبلغ عددهم 8 أشخاص، منهم 5 من الذكور، و3 من الإناث. وكان الهدف من هذه العينة جمع بيانات معمقة عن قصص الابتزاز الإلكتروني وحالاته في السلطنة.

ثانياً – عينة المقابلات الجماعية وجلسات النقاش البؤرية: وقد طبقت على عينتين، الأولى عينة من الخبراء في مجال أمن المعلومات، وهم متطوعون لمكافحة الابتزاز وجرائمه والتوعية بشأنها، بلغ عددهم 12 شخصاً: 9 من الذكور، و3 من الإناث، أما العينة الثانية فتكونت من الاختصاصيين الاجتماعيين والنفسيين بوزارة التربية والتعليم، بلغ عددهم 16 اختصاصياً واختصاصية: 3 من الذكور، و13 من الإناث. كان الهدف من أخذ هذه العينات جمع بيانات محددة ومعمقة وتفصيلية عن تحليل أسباب حالات الابتزاز الإلكتروني وأشكاله وأساليبه في السلطنة، مع المقارنة بين وجهات نظر الفريقين؛ لكون الفريق الأول يعمل مع الضحايا بشكل تطوعي غير رسمي، أما الفريق الثاني فيفترض أنه يعمل بشكل رسمي لمساعدة ضحايا الابتزاز.

أدوات الدراسة:

– **استمارة المقابلات الفردية المفتوحة:** لتحقيق أهداف الدراسة أعدّ الباحثان استمارة مقابلة مفتوحة، تكونت من قسمين: القسم الأول تكون من البيانات الشخصية عن المشاركين مثل: الجنس، والعمر، والمستوى التعليمي، أما القسم الثاني فيركز على جمع البيانات عن قصص الابتزاز الواقعية في المجتمع العماني. ويشتمل القسم الثاني على خمسة بنود رئيسة، هي: أشكال الابتزاز الإلكتروني الأكثر شيوعاً في المجتمع، والمراحل التي تمر بها عملية الابتزاز، والأسباب التي

تدفع الضحية للرضوخ لجرائم الابتزاز الإلكتروني، مدى توافر المعلومات لدى الضحايا بكيفية التعامل مع مواقف الابتزاز الإلكتروني، والمعرفة بالجهات التي يمكن أن تقدم الدعم لضحايا الابتزاز.

– **استمارة المقابلات الجماعية المقننة:** لتحقيق أهداف الدراسة ولجمع بيانات دقيقة عن حالات الابتزاز الإلكتروني في السلطنة، أعدّ الباحثان استمارة مقابلة مقننة بالاستفادة من المعلومات التي جمعها من استمارة المقابلة المفتوحة واستمارة مجموعات النقاش البؤرية، ومن الأدبيات السابقة المتعلقة بموضوع الابتزاز الإلكتروني. وقد تكونت الاستمارة من قسمين: القسم الأول تكون من البيانات عن المشاركين مثل: الجنس، والعمر، والمستوى التعليمي، والوظيفة، أما القسم الثاني فتكون من ثمانية أبعاد رئيسية، كالآتي:

– تقدير حجم انتشار ظاهرة الابتزاز الإلكتروني في المجتمع العماني: يتكون هذا البعد من فقرة واحدة، تتم الاستجابة لها وفقاً لمقياس ليكرت الخماسي؛ مراوحة بين (منتشرة بدرجة كبيرة جداً ومنتشرة بدرجة قليلة جداً).

– الفئات الأكثر عرضة للابتزاز في المجتمع العماني: تكون من 5 فقرات هي الفئات المختلفة المعرضة للابتزاز في المجتمع؛ حيث يطلب من المستجيب تقدير درجة تعرضهم للابتزاز وفقاً لمقياس ليكرت الخماسي، وتراوح الاستجابات بين (معرضون بدرجة كبيرة جداً – معرضون بدرجة قليلة جداً)، ومن أمثلة هذه الفئات: طلبة الجامعات والكليات.

– أشكال الابتزاز الإلكتروني: ويتكون هذا البعد من 5 فقرات، تشكل أبرز أشكال الابتزاز، التي يمكن أن يتعرض لها ضحايا جرائم الابتزاز الإلكتروني في السلطنة. يطلب من المستجيب تقدير درجة حدوث هذه الأشكال من الابتزاز وفقاً لمقياس ليكرت الخماسي، وتراوح الاستجابات بين (تحدث بدرجة كبيرة جداً وتحدث بدرجة قليلة جداً)، ومن أمثلة هذه الأشكال: ابتزاز ذكر لأنثى.

– الأساليب التقنية المستخدمة في الابتزاز الإلكتروني: ويتكون هذا البعد من 12 فقرة، تمثل معظم تقنيات الابتزاز. يطلب من المستجيب تقدير درجة استخدام هذه التقنيات في حالات الابتزاز وفقاً لمقياس ليكرت الخماسي، وتراوح الاستجابات بين (دائماً ونادراً)، ومن أمثلة هذه الأساليب: تصوير الضحية بكاميرا خفية.

– أسباب الوقوع في الابتزاز الإلكتروني: ويتكون هذا البعد من 7 فقرات، تمثل

معظم أسباب الابتزاز. يطلب من المستجيب تقدير درجة تكرار هذه الأسباب في حالات الابتزاز وفقاً لمقياس ليكرت الخماسي، وتراوح الاستجابات بين (دائماً ونادراً)، ومن أمثلة هذه الأسباب: تفكك أسر الضحية؛ مما يسبب شعوره بالحرمان العاطفي يُعوضه بالبحث عن بديل في ظل غياب الرقابة الوالدية والتوعية بمخاطر وسائل التقنية الحديثة.

– أسباب الرضوخ للابتزاز الإلكتروني: ويتكون هذا البعد من 6 فقرات، تمثل معظم أسباب رضوخ الضحية للابتزاز. يطلب من المستجيب تقدير درجة تكرار هذه الأسباب في حالات الابتزاز الواقعية في السلطنة وفقاً لمقياس ليكرت الخماسي، وتراوح الاستجابات بين (دائماً ونادراً)، ومن أمثلة هذه الأسباب: الخوف من إفشاء سره إذا لجأ إلى أحد.

– الآثار النفسية والاجتماعية والاقتصادية للابتزاز الإلكتروني: ويتكون هذا البعد من 14 فقرة، تمثل مختلف الآثار النفسية والاجتماعية والاقتصادية للابتزاز. يطلب من المستجيب تقدير درجة تكرار هذه الآثار في حالات الابتزاز الواقعية في السلطنة وفقاً لمقياس ليكرت الخماسي، وتراوح الاستجابات بين (دائماً ونادراً)، ومن أمثلة هذه الأسباب: فقدان الشهية.

– الإستراتيجيات الممكنة للحد من ظاهرة الابتزاز الإلكتروني: ويتكون هذا البعد من 8 فقرات، تمثل بعض الإستراتيجيات الممكنة لتفعيل دور المؤسسات التربوية في الحد من ظاهرة الابتزاز الإلكتروني. يطلب من المستجيب تقدير درجة تكرار هذه الآثار في حالات الابتزاز الواقعية في السلطنة وفقاً لمقياس ليكرت الخماسي، وتراوح الاستجابات بين (دائماً ونادراً)، ومن أمثلة هذه الأسباب: توعية المعلمين بكيفية اكتشاف ضحايا الابتزاز من خلال التغيرات التي تطرأ على سلوكهم.

– **استمارة مجموعات النقاش البؤرية:** لتحقيق أهداف الدراسة ولجمع بيانات معمقة عن حالات الابتزاز الإلكتروني في السلطنة، أعدّ الباحثان استمارة مجموعات النقاش البؤرية بالاستفادة من المعلومات التي تم جمعها من استمارة المقابلة المفتوحة ومن الأدبيات السابقة المتعلقة بموضوع الابتزاز الإلكتروني. وقد تكونت الاستمارة من قسمين: القسم الأول تكون من البيانات عن المشاركين مثل: الجنس، والعمر، والمستوى التعليمي، والوظيفة، أما القسم الثاني فتكون من خمسة محاور رئيسة على النحو الآتي:

- تقدير حجم انتشار ظاهرة الابتزاز الإلكتروني في المجتمع العماني.
- أبرز أشكال الابتزاز الإلكتروني التي يتعرض لها ضحايا جرائم الابتزاز الإلكتروني في السلطنة.
- الأسباب التي تدفع مرتكبي جرائم الابتزاز الإلكتروني للقيام بالابتزاز.
- كيفية اختيار مرتكبي جرائم الابتزاز الإلكتروني لضحاياهم.
- الآثار النفسية والاجتماعية المترتبة على الوقوع ضحية الابتزاز الإلكتروني.

الصدق والثبات:

أولاً – الصدق والثبات بالنسبة لاستمارة المقابلة الجماعية المقننة: تم التحقق من صدق استمارة المقابلة الجماعية المقننة من خلال عرضها على 5 محكمين من المتخصصين في مجال أمن المعلومات. وقد أخذ بملاحظاتهم وتعديل الاستمارة في ضوئها؛ لتظهر الاستمارة في صورتها النهائية. أما التحقق من ثبات الاستمارة، فقد تم باستخدام معامل الاتساق الداخلي Cronbach's-alpha لحساب معامل الثبات. وبلغت قيمة المعامل 0,795؛ مما يدل على تمتع استمارة المقابلة بمعامل ثبات مناسب وكاف لإجراء الدراسة.

ثانياً – الصدق والثبات بالنسبة لاستمارة المقابلة الفردية المفتوحة واستمارة مجموعات النقاش المركزة: بصفة عامة، يشير الصدق في البحوث الكيفية، على غرار البحوث الكمية، إلى درجة استقلالية الاستجابات عن الظروف العرَضية للبحث، ولكنه قد يتأتى كذلك من أمانة البيانات وعمقها وثرائها وسعتها وتعددية المصادر؛ أما الثبات فيشير إلى الحد الذي يتم فيه فهمها فهماً صحيحاً. وبالنسبة للصدق في الدراسة الحالية، تم التحقق منه من خلال عدة طرق، هي:

- الصدق الوصفي (Descriptive Validity): وذلك من خلال مراعاة الدقة في نقل شهادات الخبراء المرصودة كما هي موَثّقة (موصوفة) من قبل الباحثين. وتم ذلك من خلال تطبيق إستراتيجية التقاطع الثلاثي أو المتعدد (Triangulation) باستخدام عدة ملاحظين؛ حيث تم تسجيل جلسة النقاش البؤرية بالصوت والصورة، كما تم المقارنة بين التسجيل المدون من قبل ثلاثة ملاحظين.

- الصدق التأويلي (Interpretative Validity): وذلك من خلال مراعاة الصدق في تأويل ما تم فهمه من وجهة نظر الخبراء وآرائهم في مجال الهوية، وفهم المعاني

المرتبطة بكلمات الخبراء وأفعالهم. ويمكن التعبير عنه كذلك بالدقة في نقل تصورات الخبراء للعوامل المؤثرة على الهوية الوطنية العمانية، والتأكد من مدى تطابقها مع تأويلات الباحثين لتصوراتهم.

– الصدق النظري (Theoritical Validity): وذلك من خلال وجود تطابق بين دلالات البيانات المجمعة واتساقها مع التفسير النظري. ويمكن التعبير عن ذلك بالمعقولية النظرية للنتائج، وخاصة أنه تم الاحتكام إلى عدة نظريات لتفسير النتائج (Theory triangulation).

أما الثبات في الدراسة الحالية فقد تم التحقق منه من خلال أمرين، هما: تقدير مدى تمثيل الاستنتاجات للواقع تمثيلاً حقيقياً، وتقدير إذا ما كانت الأدوات المصممة من قبل الباحثين تقيس مقاطع حقيقية من التجربة البشرية. وبالمقابل تعمد درجة الثبات الداخلي للنتائج على اتباع التقنيات الصحيحة في جمع البيانات وتحليلها. وبالنسبة للدراسة الحالية فقد تم مراعاة اتباع التقنيات الآتية:

– الشرح المبدئي للهدف من جلسات النقاش المركزة وأهميتها، وأسلوب النقاش وقواعده.

– طرح الأسئلة أو العبارات بعناية شديدة وبلغة سهلة وواضحة.

– تلخيص التعليقات بعد مناقشة كل سؤال، والتأكد من اتفاق المشاركين عليها.

– التأكد من مشاركة الجميع في النقاش، وتشجيعهم على الحوار وعرض الخبرات الإيجابية، وعدم الاعتراض على أي إجابة أو رأي.

– عدم الانتقال إلى نقطة أو سؤال آخر قبل التأكد من الحصول على إجابة مكتملة وآراء واضحة.

– الموضوعية وعدم التأثير على المشاركين أو محاولة توجيه إجاباتهم إلى جهة معينة.

– مراجعة الأداة بشكل سريع والتأكد من تغطية كل الأسئلة أو النقاط قبل إنهاء جلسات النقاش.

– تلخيص نهائي لما دار في أثناء جلسات النقاش، وشكر المشاركين فيها على

تعاونهم وإثرائهم للجلسات النقاشية، والتأكد من إمكانية الرجوع إليهم عند الضرورة للتأكد من بعض المعلومات.

الأساليب الإحصائية:

لتحقيق أهداف الدراسة وتحليل البيانات التي جمعت بواسطة المقابلات الجماعية المقننة فقد استخدمت الأساليب الإحصائية الآتية:

– المتوسط الحسابي MeanP وذلك لمعرفة ارتفاع أو انخفاض استجابات أفراد الدراسة، وترتيب العبارات بحسب أعلى متوسط حسابي وفقاً للمعيار الآتي: 4,21–5,00 مرتفع جداً، 3,41–4,20 مرتفع، 2,61–3,40 متوسط، 1,81–2,60 منخفض، –1,00 منخفض جداً.

– الانحراف المعياري Standard Deviation؛ لتعرف انحراف استجابات أفراد الدراسة لكل عبارة عن المتوسط الحسابي لها، ويلاحظ أن الانحراف المعياري يوضح التشتت في استجابات أفراد عينة الدراسة، فكلما اقتربت قيمته من الصفر تركزت الاستجابات وانخفض تشتتها.

– اختبار (ت) لعينة واحدة T-Test؛ لتعرف إذا ما كانت هنالك فروق ذات دلالة إحصائية بين استجابات أفراد عينة الدراسة نحو أبعاد الدراسة.

أما البيانات التي جمعت بواسطة المقابلات المفتوحة ومجموعات النقاش البؤرية فقد استخدم برنامج الأطلس. تي أي 8 في ترميز وتنظيم البيانات وحساب تكراراتها، وتسهيل استجلاب الاقتباسات المتناسبة مع محاور الأسئلة.

نتائج الدراسة ومناقشتها:

أولاً – النتائج المتعلقة بالسؤال الأول ونصه: "هل توجد فروق دالة إحصائياً بين الخبراء المتطوعين للتوعية بجرائم الابتزاز الإلكتروني والاختصاصيين الاجتماعيين والنفسيين في تقديرهم لحجم انتشار الابتزاز الإلكتروني في المجتمع العماني؟". للإجابة عن هذا السؤال حسبت متوسطات الرتب ومجموعها، وقيمة (U، W، Z) باستخدام اختبار مان ويتني لمجموعتين مستقلتين للمقارنة بين آراء الفريقين، وهو ما يوضحه جدول (1).

جدول (1)
نتائج اختبار مان ويتني لمجموعتين مستقلتين لمقارنة تقدير عينتي الدراسة لحجم انتشار ظاهرة الابتزاز الإلكتروني في المجتمع العماني

المجموعة	المتوسط الكلي	الانحراف المعياري	متوسط الرتب	مجموع الرتب	قيمة U	قيمة W	قيمة Z	الدلالة الإحصائية
الخبراء المتطوعون (ن=12)	3,64	0,82	19,33	232,00	38,00	174,00	2,88	0,004
والاختصاصيون الاجتماعيون والنفسيون (ن=16)			10,88	174,00				

يتضح من جدول (1) أن المتوسط الكلي لتقدير عينتي الدراسة لحجم انتشار ظاهرة الابتزاز في المجتمع العماني 3,64، وهو أعلى من المتوسط النظري للمقياس الخماسي 3، ويمكن القول إن الظاهرة منتشرة بشكل مرتفع وفقاً لمعيار تصنيف المتوسطات الذي حددته الدراسة في الأساليب الإحصائية. وتجدر الإشارة هنا إلى أنه من الصعب تحديد نسبة انتشار الابتزاز الإلكتروني بدقة؛ وذلك لعدم توافر إحصائيات دقيقة عن حالات الابتزاز في السلطنة؛ نظراً لتحفظ الضحايا عن الإبلاغ خوفاً على السمعة، وكذلك سياسة عدم الإفصاح عن البيانات التي تتبعها كثير من المؤسسات في السلطنة. لذا ركزت الدراسة على تحديد حجم انتشار الظاهرة من خلال تقديرات الخبراء المتطوعين للتوعية بجرائم الابتزاز الإلكتروني والاختصاصيين الاجتماعيين والنفسيين؛ حيث وجدت فروق دالة إحصائياً بين تقديراتهم لحجم انتشار الظاهرة لصالح الخبراء المتطوعين للتوعية بجرائم الابتزاز، الذين يرون أن حجم انتشار الظاهرة أكبر مقارنة بتقديرات الاختصاصيين الاجتماعيين والنفسيين. ويعود ذلك إلى عدة أسباب، منها: أن ضحايا الابتزاز يفضلون اللجوء إلى الجهات التطوعية غير الرسمية للتبليغ عن جرائم الابتزاز التي يتعرضون لها؛ طلباً للمساعدة وذلك خوفاً من انتشار الخبر وتأثر سمعتهم أو تحويل القضية للشرطة والادعاء، أما السبب الآخر فيعود لكونهم يفضلون حل المشكلة بشكل تقني من خلال الخبراء بحذف الرابط أو الصور والفيديو التي أدت إلى ابتزازهم. وتأكيداً لهذه النتيجة قال أحد المشاركين: "الابتزاز الإلكتروني ظاهرة منتشرة بشكل كبير في المجتمع يرتكبها أفراد أو عصابات إلكترونية، ويتم من خلالها استهداف أشخاص بشكل عشوائي؛ بحيث يتم التواصل معهم باستخدام

حسابات زائفة وتكوين صداقات معهم، وذلك عن طريق برامج المحادثات والفيديوهات. وليس من السهل تحديد نسبة انتشارها في المجتمع؛ لأن الكثير من الضحايا لا يبلغون عنها خوفاً من وصمة العار، هذا فضلاً عن كون الجهات الرسمية تتعامل مع الحالات بشكل سري، وتتبع سياسة عدم الإفصاح عن البيانات".

ثانياً – النتائج المتعلقة بالسؤال الثاني ونصه: "هل توجد فروق دالة إحصائياً بين الخبراء المتطوعين للتوعية بجرائم الابتزاز الإلكتروني والاختصاصيين الاجتماعيين والنفسيين في تقديرهم أي فئات المجتمع هي الأكثر عرضة لجرائم الابتزاز الإلكتروني؟". للإجابة عن هذا السؤال حسبت متوسطات الرتب ومجموعها، وقيمة (U، W، Z) باستخدام اختبار مان ويتني لمجموعتين مستقلتين للمقارنة بين آراء الفريقين بالنسبة للفئات المختلفة، وهو ما يوضحه جدول (2).

جدول (2)
نتائج اختبار مان ويتني لمجموعتين مستقلتين لمقارنة تقدير عينتي الدراسة أي فئات المجتمع العماني هي الأكثر عرضة لجرائم الابتزاز الإلكتروني

الفئات	المتوسط الكلي	الانحراف المعياري	المجموعة	متوسط الرتب	مجموع الرتب	قيمة U	قيمة W	قيمة Z	الدلالة الإحصائية
طلبة الجامعات والكليات	4,14	0,80	الخبراء المتطوعون (ن=12)	17,04	204,50	65,50	201,50	1,53	0,125
			والاختصاصيون الاجتماعيون والنفسيون (ن=16)	12,59	201,50				
طلبة المدارس (11 – 18) سنة	3,85	1,00	الخبراء المتطوعون (ن=12)	15,92	191,00	79,00	215,00	0,83	0,406
			والاختصاصيون الاجتماعييو والنفسيون (ن=16)	13,44	215,00				
الموظفون بالقطاعين العام والخاص	3,32	1,24	الخبراء المتطوعون (ن=12)	19,71	236,50	33,50	169,50	3,03	0,002
			والاختصاصيون الاجتماعيون والنفسيون (ن=16)	10,59	169,50				
المشاهير والأغنياء	3,32	1,61	الخبراء المتطوعون (ن=12)	16,13	193,50	76,50	212,50	0,93	0,351
			والاختصاصيون الاجتماعيون والنفسيون (ن=16)	13,28	212,50				

تتابع/ جدول (2)
نتائج اختبار مان ويتني لمجموعتين مستقلتين لمقارنة تقدير عينتي الدراسة أي فئات المجتمع العماني هي الأكثر عرضة لجرائم الابتزاز الإلكتروني

الفئات	المتوسط الكلي	الانحراف المعياري	المجموعة	متوسط الرتب	مجموع الرتب	قيمة U	قيمة W	قيمة Z	الدلالة الإحصائية
الأطفال (5 – 10) سنوات	2,67	1,65	الخبراء المتطوعون (ن=12)	17,42	209,00	61,00	197,00	1,67	0,095
			والاختصاصيون الاجتماعيون والنفسيون (ن=16)	12,31	197,00				
المتقاعدون	2,64	1,20	الخبراء المتطوعون (ن=12)	17,75	213,00	57,00	193,00	1,86	0,062
			والاختصاصيون الاجتماعيون والنفسيون (ن=16)	12,06	193,00				

يتضح من جدول (2 ترتيب المتوسطات الكلية لمختلف الفئات المعرضة للابتزاز في المجتمع؛ حيث كانت فئة طلبة الجامعات والكليات هي الفئة الأكثر عرضة للابتزاز الإلكتروني، تلتها فئة طلبة المدارس، ثم الموظفون بالقطاعين العام والخاص والمشاهير بالدرجة نفسها، ثم الأطفال دون العاشرة، وأخيراً المتقاعدون. ويمكن تفسير هذه النتيجة في ضوء طبيعة المراحل العمرية للفئات المختلفة؛ حيث يكون الشباب معرضين للظاهرة بشكل أكبر؛ نظراً لاستخدامهم الواسع لشبكات المعلومات ووسائل التواصل الاجتماعي، ونظراً لاستجابتهم بشكل أكبر للمغريات وعدم نضوجهم الانفعالي والنفسي.

كذلك تشير النتائج في جدول (2) إلى عدم وجود فروق دالة إحصائياً بين تقديرات الخبراء المتطوعين للتوعية بجرائم الابتزاز الإلكتروني والاختصاصيين الاجتماعيين والنفسيين للفئات الأكثر عرضة للابتزاز إلا فيما يتعلق بفئة الموظفين بالقطاعين العام والخاص؛ حيث يرى الخبراء المتطوعون أنهم الأكثر عرضة للابتزاز؛ لكونهم يملون المال الذي يستهدفه المبتزون. والجدير بالذكر هنا أن المشاركين في مجموعات النقاش المركزة أضافوا فئات أخرى معرضة للابتزاز، منها: الباحثون عن عمل، وربات المنازل، والعاملات في المنازل، وذوو الاحتياجات الخاصة، مؤكدين أنه لا توجد فئة في المجتمع غير معرضة للابتزاز.

وتأكيداً للنتيجة السابقة قال أحد المشاركين في مجموعات النقاش البؤرية: "الجميع معرض لهذه الجريمة وبخاصة المراهقون؛ كونهم يمرون بمرحلة صعبة في حياتهم؛ حيث يجدون صعوبة في التفريق بين الصحيح والخاطئ، ويقومون بالأعمال التي يرغبون بها دون التفكير بالعواقب والنتائج".

وتتفق نتائج الدراسة الحالية مع دراسة الغامدي وعبده (2016)، التي وجدت أن طلبة الجامعات من أكثر الفئات العمرية عرضة للابتزاز الإلكتروني، بينما تختلف مع دراسة كوبسكي (Kopecky, 2017)، التي وجدت أن الأطفال من أكثر الفئات عرضة للابتزاز لصغر سنهم وعدم إدراكهم لكيفية التصرف في حالة التعرض للابتزاز.

ثالثاً – النتائج المتعلقة بالسؤال الثالث، ونصه: "ما أبرز أشكال الابتزاز الإلكتروني التي يتعرض لها ضحايا جرائم الابتزاز الإلكتروني في السلطنة؟". للإجابة عن هذا السؤال حسبت المتوسطات والانحرافات المعيارية لآراء جميع المشاركين في المقابلات الجماعية المقننة، حول تقديرهم لدرجة شيوع الأشكال المختلفة للابتزاز في المجتمع العماني ثم تم حساب قيمة (ت) لعينة واحدة والدلالة الإحصائية لكل شكل من أشكال الابتزاز باستخدام القيم المحسوبة للوسط الفعلي والنظري وهو 3، على نحو ما يوضحه جدول (3).

جدول (3)
نتائج مقارنة المتوسطات الفعلية مع المتوسطات النظرية لأشكال الابتزاز الإلكتروني في السلطنة (ن=28)

أشكال الابتزاز الإلكتروني	المتوسط الفعلي	الانحراف المعياري	قيمة ت	الدلالة الإحصائية
ابتزاز ذكر لأنثى	4,07	1,01	5,58	0,000
ابتزاز أنثى لأنثى	3,25	1,29	1,02	0,316
ابتزاز (عصابة/ منظمة خارجية) لضحايا متنوعين	3,21	1,25	0,90	0,750
ابتزاز ذكر لذكر	3,21	0,99	1,14	0,264
ابتزاز أنثى لذكر	2,89	1,03	0,55	0,587

يظهر من جدول (3) أن جميع المتوسطات الحسابية لأشكال الابتزاز غير دالة

إحصائياً عند مستوى دلالة أقل من 0,05 ما عدا ابتزاز ذكر لأنثى. وقد كانت المتوسطات الفعلية لجميع أشكال الابتزاز أعلى من المتوسط النظري ما عدا ابتزاز أنثى لذكر، فقد كان أقل من المتوسط النظري. وأظهرت النتائج أن أكثر أشكال الابتزاز الإلكتروني شيوعاً في المجتمع العماني – بحسب تقدير المشاركين في الدراسة – ابتزاز ذكر لأنثى، يليه ابتزاز أنثى لأنثى، ثم ابتزاز (عصابة/ منظمة خارجية) لضحايا متنوعين، يليه ابتزاز ذكر لذكر، وأخيراً ابتزاز أنثى لذكر. وقد أكد المشاركون في جلسات النقاش البؤرية أن أكثر حالات الابتزاز التي تأتي من داخل السلطنة هي ابتزاز الفتيات من قبل الذكور؛ حيث يتم استدراج الفتيات من خلال وسائل التواصل إلى أن تتطور العلاقة ثم يطلب المبتز من الفتاة إرسال صور لها وأحياناً تتطور العلاقة لأكثر من ذلك، وفي حال أن الفتاة استجابت، ثم أرادت الانسحاب من العلاقة يقوم المبتز بالضغط عليها من خلال الصور ومقاطع الفيديو التي يمتلكها، ثم يقوم بتهديدها بنشر صورها أو إرسالها إلى عائلتها حتى تستمر في هذه العلاقة. أما أقل أشكال الابتزاز شيوعاً فهو ابتزاز أنثى لذكر؛ ويعود السبب في ذلك إلى الطبيعة النفسية للمرأة، وإلى طبيعة المجتمع العماني والعربي عموماً، الذي غالباً ما يفرض على المرأة من القيود الاجتماعية والرقابة ما لا يفرضه على الرجل.

وقد ذكر المشاركون في مجموعات النقاش المركزة أشكالاً أخرى من الابتزاز غير تلك المحددة في استمارة المقابلات الجماعية المقننة، ومنها: ابتزاز بالغ لطفل، وابتزاز طفل لطفل أصغر منه، وابتزاز عماني لوافد، وابتزاز وافد لعماني.

رابعاً – النتائج المتعلقة بالسؤال الرابع ونصه: "ما أهم الأساليب التقنية المستخدمة في الابتزاز الإلكتروني؟" للإجابة عن هذا السؤال حسبت المتوسطات والانحرافات المعيارية لآراء جميع المشاركين في المقابلات الجماعية المقننة، حول تقديرهم لدرجة شيوع استخدام الأساليب التقنية للابتزاز في المجتمع العماني، ثم حسبت قيمة (ت) لعينة واحدة والدلالة الإحصائية لكل أسلوب من أساليب الابتزاز باستخدام القيم المحسوبة للمتوسط الفعلي والنظري، الذي بلغ 3، على نحو ما يوضحه جدول 4.

جدول (4)
نتائج مقارنة المتوسطات الفعلية مع المتوسطات النظرية لأهم الأساليب التقنية المستخدمة في الابتزاز الإلكتروني

أساليب الابتزاز	المتوسط الفعلي	الانحراف المعياري	قيمة ت	الدلالة الإحصائية
1 – إرسال طلب صداقة للضحايا عبر مواقع التواصل الاجتماعي	4,07	0,60	9,38	0,000
2 – إرسال طلب محادثة فيديو مرئي لفتاة في صور جميلة ومغرية	3,96	0,63	8,00	0,000
3 – جمع بيانات عن الضحية من خلال بياناته في مواقع التواصل الاجتماعي	3,85	0,59	7,67	0,000
4 – تصيد الضحايا عبر إرسال بريد إلكتروني عشوائي	3,78	0,83	4,99	0,000
5 – استهداف مستخدمي المواقع الإباحية	3,71	0,71	5,30	0,000
6 – اختراق حاسوب الضحية وتصويره عبر كاميرا الإنترنت	3,42	0,95	2,36	0,026
7 – استخدام برامج التجسس على الحواسيب والهواتف	3,39	1,16	1,78	0,086
8 – استخدام محركات بحث متخصصة لجمع بيانات عن الضحايا	3,32	1,12	1,51	0,142
9 – تصوير الضحية بكاميرا خفية	3,28	0,76	1،98	0,058
10 – استخدام تقنية البلوتوث والأير درب /Bluetooth AirDrop	3,10	0,83	0,68	0,501
11 – تعقب الضحية عبر GPS	2،78	1,19	0,94	0,352
12 – استخدام الميكروفونات بعيدة المدى	2,71	1,18	1،27	0,212

يظهر من جدول (4) أن المتوسطات الفعلية لجميع أساليب الابتزاز أعلى من المتوسط النظري ما عدا تعقب الضحية عبر GPS، واستخدام الميكروفونات بعيدة المدى، فقد كان أقل من المتوسط النظري. كما يظهر أن الأساليب التقنية للابتزاز التي كانت المتوسطات المحسوبة لها دالة إحصائياً عند مستوى دلالة أقل من 0,05

هي سبعة أساليب من ضمن الاثني عشر أسلوباً في جدول 4. وقد جاء ترتيبها من حيث درجة الشيوع على النحو الآتي: إرسال طلب صداقة للضحايا عبر مواقع التواصل الاجتماعي، يليه إرسال طلب محادثة فيديو مرئي لفتاة في صور جميلة ومغرية، ثم جمع بيانات عن الضحية من خلال بياناته في مواقع التواصل الاجتماعي، ثم تصيد الضحايا عبر إرسال بريد إلكتروني عشوائي، ثم استهداف مستخدمي المواقع الإباحية، ثم اختراق حاسوب الضحية وتصويره عبر كاميرا الإنترنت، وأخيراً تصوير الضحية بكاميرا خفية. وتأكيداً لما سبق قال أحد الخبراء المشاركين في مجموعات النقاش المركزة: "إن الأساليب المتبعة في حالات الابتزاز الإلكتروني في السلطنة يمكن أن تصنف إلى نوعين: النوع الأول يصنف ضمن الجريمة المنظمة، أما النوع الثاني فيصنف كجريمة شخصية. النوع الأول تديره عصابات دولية محترفة، معظمها من الفلبين والمغرب ونيجيريا؛ حيث لا توجد اتفاقيات مع الإنتربول معها، وهذا النوع أكثر خطورة؛ نظراً لأن جرائمه مخطط لها بشكل محكم ويتم اختيار الضحايا بعناية شديدة، ويستخدمون أساليب تقنية متعددة عن طريق إرسال طالب صداقة بشكل مغر يقدمه المحتال كطعم، ويتم من خلالها اصطياد الضحية، وإيقاعها في فخ الابتزاز. ومن الأساليب التي يستخدمونها ما يسمى بالهندسة الاجتماعية؛ حيث توضع الضحية تحت المجهر ويراقبونه، ويتابعون حساباته ليعرفوا اتجاهاته وميوله، ويجمعون كل المعلومات الكافية عنه، ثم يرمون الطعم الذي يكون غالباً فتاة جميلة مثيرة، ترسل له طلب إضافة أو متابعة، فيوافق ويقبل، وتبدأ بعدها عملية تهديده بالفيديو المسجل عليه وابتزازه بشكل متواصل".

وتتفق نتائج الدراسة الحالية مع نتائج دراستي دراسة آل النمر (2013)، ودراسة رامدينماوي، وآخرون (Ramdinmawii, et al., 2014)؛ حيث تطرقتا إلى مدى تطور تقنيات الابتزاز الإلكتروني، وضرورة تطور طرق الكشف عنها من قبل السلطات الرسمية.

خامساً – النتائج المتعلقة بالسؤال الخامس ونصه: "كيف تتطور حالات الابتزاز الإلكتروني؟ وما المراحل التي تمر بها؟". وقد تمت الإجابة عن هذا السؤال من خلال تحليل آراء المشاركين في المقابلات الفردية المفتوحة وتحليل قصص حالات الابتزاز الإلكتروني الواقعية التي تعاملوا معها، وقد أظهرت النتائج أن عملية الابتزاز تمر – بشكل عام – بالمراحل الآتية: **مرحلة الطلب**؛ حيث يقوم المبتز بطلب

الحديث أو تبادل الرسائل الإلكترونية أو الاستشارة والنقاش والاستفسار من الضحية، تليها **مرحلة مقاومة الطلب**؛ وتبدأ عندما يقوم الضحية برفض الحديث أو استمرار التواصل مع المبتز، ومحاولة قطع العلاقة معه ثم تبدأ **مرحلة الضغط**؛ حيث يقوم المبتز بتكرار الطلب بإلحاح شديد وبالضغط المستمر بشتى الوسائل والطرق اللبقة المتاحة، فإن لم يستجب تبدأ بعدها **مرحلة التهديد**؛ حيث يتم تهديد الضحية بفضح العلاقة ونشر صور بينهما أو نشر معلومات سرية عن الضحية، وأحياناً يتم التهديد بالتشهير بالضحية عبر معلومات غير حقيقية ولكنها تجعل الضحية يرضخ للتهديد خوفاً من تشويه سمعته، وهنا تبدأ **مرحلة الإذعان للتهديد** فينفذ الضحية ما يطلبه المبتز؛ وذلك بدفع المال أو بالقيام بأعمال يطلبها المبتز، وعادة ما تكون أعمالاً لا أخلاقية، وبعدها تبدأ **مرحلة التكرار**، وتتمثل الاقتباسات الدالة على كل مرحلة من أقوال المشاركين الآتية:

"يستخدم المبتزون في البداية طلب صداقة من خلال وسائل عدة، أهمها مواقع التواصل الاجتماعي مثل سي هاي، وسناب شات، والانستجرام، والواتس أب والفيس بوك، والبريد الإلكتروني، إلى أن يتطور الوضع لاستخدام برامج أخرى تتيح استخدام محادثات الفيديو ويتم بعدها تصوير الضحية في وضع مسيء".

"بعد أن يمتلك المبتز صوراً أو فيديو فاضحاً للضحية يبدأ الابتزاز، ونجد بعض الضحايا يقاومون في البداية؛ مما يجعل المبتز يضغط على الضحية بنشر جزء من الصور والمقاطع في اليوتيوب، ليثبت للضحية قدرته على فضحه وتدمير سمعته".

"عندما يتملك الخوف والقلق والاضطراب الضحية بعد التهديد المستمر يبدأ بالرضوخ للابتزاز خوفاً على سمعته أو حياته الزوجية أو وظيفته، فيبدأ بإرسال المال للمبتز أو تنفيذ الأوامر التي يصدرها له مهما كانت صعبة أو مذلة".

"يعتقد معظم الضحايا بأن الابتزاز سينتهي عندما يرسل المبلغ للضحية ولكن يكرر عملية الابتزاز كلما احتاج للمال؛ حيث يصبح الضحية هو مصدر الرزق له ولا يتركه حتى يستنزف جميع أمواله".

"تبدأ معظم حالات الابتزاز بتسرب بعض المعلومات أو الصور للضحية ووصولها للمبتز سواء بعلم الضحية أو من دون علمه. يقوم بعدها المبتز بالتواصل مع الضحية وتهديده بنشر هذه المعلومات في حالة عدم إرسال مبالغ مالية أو القيام

بأعمال معينة. وقد يستمر الابتزاز لفترات طويلة في حالة رضوخ الضحية وعدم إبلاغه للجهات الرسمية، وأعرف شخصياً حالة استمرت عملية ابتزازها لمدة ثلاث سنوات وبعض الحالات ابتزت لفترة لأكثر من ذلك".

سادساً – النتائج المتعلقة بالسؤال السادس، ونصه: "ما مدى وعي الشباب العماني بكيفية التعامل مع مواقف الابتزاز الإلكتروني؟". وقد تمت الاجابة عن هذا السؤال من خلال تحليل آراء المشاركين في المقابلات الفردية المفتوحة، وقد أظهرت النتائج أن 60% من المشاركين يرون أن وعي الشباب بكيفية التعامل مع مواقف الابتزاز لا يزال دون المأمول، وأن هناك قلة في الوعي بشكل خاص لدى فئة الإناث، بينما يرى 40% منهم أن الوعي موجود ولكن التطبيق للمعرفة غير موجود. وتتمثل الاقتباسات الدالة على هذه النتيجة في مثل أقوال المشاركين الآتية: "من خلال خبرتي في التعامل مع حالات الابتزاز وجدت أن 20% فقط من الحالات استطاعت التعامل مع حالات الابتزاز بشكل صحيح من خلال الإبلاغ الفوري عن الحالة وتسليمها للمختصين مع تزويدهم بجميع تفاصيل الحالة ليتمكنوا من التعامل مع المبتز بشكل مناسب، أما 80% من الحالات فقد قاموا بالإبلاغ بعد أن تطورت الحالة واضطروا لدفع مبالغ كبيرة من المال للمبتز، وحتى عندما أبلغوا الجهات المختصة لم يقدموا لهم معلومات دقيقة وكاملة عن الحالة واتبعوا سياسة اللف والدوران مما صعب عملية التعامل مع الحالة".

"أرى أن هناك قلة في وعي الشباب بالتعامل مع مواقف الابتزاز وعلى وجه الخصوص الفتيات".

"أعتقد أن المعرفة أصبحت موجودة لدى الشباب حول الابتزاز ولكن التطبيق لا يتم؛ وذلك بسبب الثقة الزائدة بالنفس، وحب الاستكشاف والفضول، والرغبة في التحدي".

وبالمقابل قال أحد المشاركين: "أرى أن حملات التوعية الكثيرة التي قدمت عن الابتزاز مثل (بلغ وسرك في بير)، و(توثق)، و(مبتز ولا أنحني)، و(والله نستاهل)، وغيرها من الحملات – جعلت مستوى وعي الشباب بالتعامل مع الابتزاز يزداد".

سابعاً – النتائج المتعلقة بالسؤال السابع، ونصه: ما مدى كفاية الجهود الحكومية والتطوعية في توعية الشباب العماني بجرائم الابتزاز الإلكتروني؟. تمت

الاجابة عن هذا السؤال من خلال تحليل آراء المشاركين في المقابلات الفردية المفتوحة، وقد أظهرت النتائج أن 80% من المشاركين يرون أنه على الرغم من أن هناك كثيراً من الجهود المبذولة من مختلف الجهات للتوعية بمخاطر الابتزاز الإلكتروني فإن هذه الجهود متفرقة وغير متكاملة؛ مما يقلل من فعاليتها ويحد من نتائجها بعيدة المدى، والدليل على ذلك تزايد عدد الحالات، وقد أكدوا جميعهم أهمية تكامل جهود مختلف الجهات بما فيها المركز الوطني للسلامة المعلوماتية، وشرطة عمان السلطانية والادعاء العام والمؤسسات التربوية، وهيئة تنظيم الاتصالات والحملات التطوعية الأهلية لمكافحة ظاهرة الابتزاز؛ حيث إن تكاتف هذه الجهات وتوحيد جهودها سيعظم من النتائج المحرزة في مجال مكافحة الابتزاز الإلكتروني. وبالمقابل يرى 20% من المشاركين أن الجهود كافية ولكن استجابة المواطنين لها ليست بالمستوى المطلوب. وتتمثل الاقتباسات الدالة على هذه النتيجة في أقوال المشاركين الآتية:

"نحتاج إلى توحيد الجهود بين مختلف الجهات، وزيادة التوعية؛ بحيث تبدأ من صفوف ما قبل المدرسة، كما نحتاج إلى زيادة المحتوى التقني في المدارس، والتوعية بأمن المعلومات، وكيفية التعامل مع أجهزة التكنولوجيا الحديثة لدى الكبار والصغار"

"من وجهة نظري الجهود مبذولة من مختلف الجهات الرسمية كافية سواء من المدارس أو الجهات الحكومية كالشرطة والادعاء وهيئة تقنية المعلومات كافية، ولكن على الرغم من ذلك نجد أن حالات الابتزاز في تزايد مستمر؛ وذلك لأن كثيراً من المواطنين لا يستمعون باهتمام لبرامج التوعية المقدمة لاعتقادهم باستحالة تعرضهم للابتزاز، وهذا السبب في وقوع كثير من الضحايا في هذا الموضوع".

ثامناً – النتائج المتعلقة بالسؤال الثامن: "ما الآثار النفسية والاجتماعية والاقتصادية المترتبة على الوقوع ضحية الابتزاز الإلكتروني؟" للإجابة عن هذا السؤال حسبت المتوسطات والانحرافات المعيارية لآراء جميع المشاركين في المقابلات الجماعية المقننة، حول تقديرهم دوافع وأسباب كل من المبتز والضحية للقيام أو الرضوخ لجرائم الابتزاز الإلكتروني ثم تم حساب قيمة (ت) لعينة واحدة والدلالة الإحصائية لكل دافع وسبب الابتزاز باستخدام القيم المحسوبة للوسط الفعلي والنظري وهو 3، على نحو ما يوضحه جدول (5).

جدول (5)
نتائج مقارنة المتوسطات الفعلية مع المتوسطات النظرية للآثار النفسية والاجتماعية والاقتصادية لجرائم الابتزاز الإلكتروني

الإستراتيجيات	المتوسط الفعلي	الانحراف المعياري	قيمة ت	الدلالة الإحصائية
أولاً – الآثار النفسية للابتزاز:				
الخوف والقلق المستمر من عواقب الابتزاز	4,25	1,07	6,14	0,00
عدم القدرة على القيام بممارسات الحياة اليومية (الوظيفة/ الدراسة)	4,10	0,68	8,54	0,00
الشرود والسرحان بسبب التفكير الدائم	4,07	0,85	6,61	0,00
الوسواس القهري الناتج عن الرعب من التهديد	4,00	0,72	7,34	0,00
فقدان الشهية	3,85	0,70	6,43	0,00
انعدام النوم	3,85	0,65	6،97	0,00
ثانياً – الآثار الاجتماعية للابتزاز:				
إفساد قيم المجتمع وأخلاقياته	3,89	0,83	5,68	0,00
تفكك الأسرة ووقوع حالات طلاق	3,75	0,64	6,14	0,00
ضعف الإنتاجية أفراد المجتمع	3,75	0,84	4,70	0,00
انتشار جرائم أخرى ذات صلة بجريمة الابتزاز مثلاً: (الدعارة، والسرقة، والقتل، ...إلخ)	3,64	1,09	3,10	0,004
حدوث حالات الانتحار	3,57	1,03	2,92	0,007
ثانياً – الآثار الاقتصادية:				
توقف الضحية عن العمل أو الدراسة	4,25	1,07	6،53	0,00
استنزاف أموال الضحية	4,14	0,89	6,78	0,00
لجوء الضحية للسرقة	4,03	0,79	6,91	0,00

يظهر من جدول (5) أن جميع آثار الابتزاز كانت المتوسطات المحسوبة لها دالة إحصائياً عند مستوى دلالة أقل من 0,05، وجميعها أعلى من المتوسط النظري.

ويمكن ترتيبها من تأثير كل منها وفق التسلسل التنازلي الظاهر في جدول 5؛ بمعنى أن أهم الآثار النفسية هي الخوف والقلق. أما الآثار الاجتماعية فكان أهمها إفساد قيم المجتمع. أما الآثار الاقتصادية فكان أهمها توقف الضحية عن الإنتاجية. وتأكيداً لهذه النتيجة قال أحد المشاركين في مجموعات النقاش البؤرية: "إن تكتم الضحية قد يؤثر عليه نفسياً فيتدنى مستواه الإنتاجي أو الدراسي إذا كان طالباً، وقد يلجأ البعض للانتحار خوفاً من الفضيحة والعار، وفي حالة رفض الضحية وعدم التعاون مع المبتز قد يتم تشويه سمعته؛ مما يؤثر على صورته في المجتمع". وقال مشارك آخر: "من عواقب الابتزاز الإلكتروني الضغوط النفسية الشديدة الناتجة من القلق والخوف، وقد يصل البعض لحالات من الاكتئاب الشديدة قد تؤدي للانتحار، أما آثاره الاجتماعية فتتمثل في كونه يفسد العلاقات الاجتماعية؛ حيث يسبب حالات من الطلاق". ومن الجدير بالذكر أن المشاركين في مجموعات النقاش البؤرية قد أضافوا آثاراً نفسية أخرى للابتزاز، منها: الاضطراب النفسي، الاكتئاب، وانفصام الشخصية.

وتتفق هذه النتائج مع عدد من الدراسات (Gómeza & Ganuza, 2002; Liua, 2010)، التي وجدت أن الابتزاز الإلكتروني جريمة تهز كيان المجتمع واستقراره، وتخلف آثاراً نفسية واجتماعية واقتصادية على الفرد والمجتمع.

تاسعاً – النتائج المتعلقة بالسؤال التاسع، ونصه: "ما الإستراتيجيات الممكنة لتفعيل دور المؤسسات التربوية في الحد من ظاهرة الابتزاز الإلكتروني؟". للإجابة عن هذا السؤال حسبت المتوسطات والانحرافات المعيارية لآراء جميع المشاركين في المقابلات الجماعية المقننة، حول الإستراتيجيات الممكنة لتفعيل دور المؤسسات التربوية في الحد من ظاهرة الابتزاز الإلكتروني، ثم حسبت قيمة (ت) لعينة واحدة والدلالة الإحصائية لكل إستراتيجية باستخدام القيم المحسوبة للوسط الفعلي والنظري وهو 3، على نحو ما يوضحه جدول (6)

جدول (6)
نتائج مقارنة المتوسطات الفعلية مع المتوسطات النظرية لإستراتيجيات الحد من الابتزاز الإلكتروني

الإستراتيجيات	المتوسط الفعلي	الانحراف المعياري	قيمة ت	الدلالة الإحصائية
– عمل حملات توعية مكثفة حول الابتزاز وطرق الوقاية منه	4,85	0,44	21,91	0,000
– توعية المعلمين حول كيفية اكتشاف ضحايا الابتزاز من خلال تغير سلوكياتهم	4,67	0,54	16,20	0,000
– قيام المؤسسات التربوية بتوعية أولياء الأمور حول أخطار الابتزاز وكيفية الوقاية منه	4,64	0,73	11,89	0,000
– تعريف أولياء الأمور ببرامج الحماية الوالدية parental control التي تضبط استخدام الأبناء للأجهزة الإلكترونية	4,64	0,55	15,55	0,000
– تدريب الاختصاصيين الاجتماعيين والنفسيين على التعامل مع ضحايا الابتزاز	4,60	0,56	15,00	0,000
– تنفيذ برامج وقائية للطلبة الأكثر عرضة للابتزاز من خلال كثرة مشكلاتهم السلوكية	4,55	0،64	12,61	0,000
– عمل دليل إرشادي للوقاية من تعرض الطلبة لجرائم المعلوماتية	4,51	0،75	10,47	0,000
– تركيز مادة تقنية المعلومات على مخاطر سوء استخدام التقنية، ووسائل التواصل الاجتماعي والجرائم المرتبطة بها	4,39	0،75	9,73	0,000

يظهر من جدول (6) أن جميع إستراتيجيات الحد من الابتزاز كانت المتوسطات المحسوبة لها دالة إحصائياً عند مستوى دالة أقل من 0,05، وكانت جميع المتوسطات أعلى من المتوسط النظري، ويمكن ترتيبها من حيث درجة أهميتها وفق التسلسل التنازلي الظاهر في جدول 6؛ بمعنى أن أهم إستراتيجية للحد من الابتزاز الإلكتروني هي عمل حملات مكثفة للتوعية حول الابتزاز الإلكتروني وطرق الوقاية منه. وتأكيداً لهذه النتيجة قال أحد المشاركين في مجموعات النقاش البؤرية: "أعتقد أن من أهم الطرق لتجنب الابتزاز الإلكتروني والحد منه، توعية

الشباب بعدم نشر البيانات الشخصية والصور والأخبار عن حياتهم الأسرية في مواقع التواصل الاجتماعي، وكذلك عدم إرسال الصور الشخصية لأشخاص مجهولين مهما كانت الأسباب، وعدم مشاركتهم معلومات خاصة وسرية، وتجنب الرد على أية رسائل مجهولة، والانتباه من بعض الروابط المشبوهة وعدم فتحها".

التوصيات:

في ضوء النتائج السابقة توصي الدراسة الحالية بإعداد خطة إجرائية للمؤسسات التربوية لتوعية الشباب حول الابتزاز الإلكتروني تتضمن:

– تكثيف حملات التوعية للشباب في المؤسسات التربوية حول الابتزاز الإلكتروني وكيف التصرف عند الوقوع فيه.

– إعداد دليل إرشادي لمكافحة الابتزاز الإلكتروني، يوزع على الشباب في المؤسسات التربوية: ويتضمن الدليل البنود الآتية: إرشادات التعامل الآمن مع الإنترنت ووسائل التواصل الاجتماعي، والتعريف بمفهوم الابتزاز وطرقه وأشكاله، ودوافع الابتزاز، ومراحله، وكيفية التصرف في حالة التعرض للابتزاز، وقصص واقعية عن حالات تعرضت للابتزاز.

– تدريب الاختصاصيين الاجتماعيين والنفسيين على التعامل مع ضحايا الابتزاز، وتزويدهم ببرامج وقائية للطلبة الأكثر عرضة للابتزاز نظراً لمشكلاتهم السلوكية.

– توعية المعلمين حول كيفية اكتشاف ضحايا الابتزاز من خلال تغير سلوكياتهم.

– توعية أولياء الأمور حول أخطار الابتزاز وكيفية الوقاية منه، وتعريفهم ببرامج الحماية الوالدية parental control التي تضبط استخدام الأبناء للأجهزة الإلكترونية.

– تضمين المناهج الدراسية للمعلومات الكافية عن خطورة الابتزاز والجهات التي يمكن اللجوء إليها طلباً للمساعدة.

المراجع:

آل النمر، محمد منصور يحيى. (2013). دور تقنية المعلومات في مكافحة جرائم الابتزاز، رسالة ماجستير "غير منشورة". جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، قسم العلوم الشرطية.

البداينة، ذياب موسى. (سبتمبر، 2014). الجرائم الإلكترونية: المفهوم والأسباب. ورقة مقدمة في الملتقى العلمي "الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية"، 2–4 سبتمبر 2014، عمان، الأردن.

حميد، صالح. (مارس، 2011). "الابتزاز: المفهوم والواقع". ورقة مقدمة في ندوة الابتزاز (المفهوم– الأسباب– العلاج)، 7–8 مارس 2011، جامعة الملك سعود، المملكة العربية السعودية.

الصالح، نزار حسين. (مارس، 2011). آثار الابتزاز على الفرد والمجتمع. ورقة مقدمة في ندوة الابتزاز (المفهوم، الأسباب، العلاج)، 7–8 مارس 2011، جامعة الملك سعود، المملكة العربية السعودية.

العيد، نوال. (مارس، 2011). الابتزاز: المفهوم، الأسباب، العلاج. ورقة مقدمة في ندوة الابتزاز (المفهوم، الأسباب، العلاج)، 7–8 مارس 2011، جامعة الملك سعود، المملكة العربية السعودية.

الغامدي، سعيد بن أحمد آل شويل؛ عبده، أشرف علي السيد. (2017). **الابتزاز الجنسي لدى شباب منطقة الباحة. من موقع:** https://www.researchgate.net/file.PostFileLoader.html? **بتاريخ 25 مايو 2017.**

الفالح، منى إبراهيم. (مارس، 2011). دور وزارة التربية والتعليم في مواجهة الابتزاز. ورقة مقدمة في ندوة الابتزاز (المفهوم، الأسباب، العلاج)، 7–8 مارس 2011، جامعة الملك سعود، المملكة العربية السعودية.

المطلق، نورة. (2016). **ابتزاز الفتيات: أحكامه** وعقوبته في الفقه الإسلامي. من موقع: https://units.imamu.edu.sa/colleges/sharia/AcademicDepts/Pages/alfeqh/entag/29.aspx بتاريخ 28 مايو 2017.

المقبالي، صلاح خليفة. (2016). **الابتزاز الإلكتروني: كيف تتجنبه؟ وماذا تفعل إذا وقعت ضحية له؟** من موقع: http://www.atheer.om بتاريخ 24 مايو 2017.

هيئة تقنية المعلومات. (2017). من موقع: http://www.ita.gov.om/ITAPortal_AR/Government/Government_Projects.aspx?NID=128 بتاريخ 15 مايو 2017.

الوطن. (19 أكتوبر، 2016). **ختام الحملة التوعوية بمخاطر الابتزاز الإلكتروني (بلغ وسرك في بئر).** تم الرجوع عبر http://alwatan.com/details/145870 بتاريخ 11 يونيو 2017.

Gómeza, F., Ganuza, J. J. (2002). Civil and criminal sanctions against blackmail: an economic analysis. *International Review of Law and Economics*, 21, 475-498.

Kopecky. K. (2017). Online blackmail of Czech children focused on so-called ''sextortion'' (analysis of culprit and victim behaviors). *Telematics and Informatics*, 34, 11-19.

Liua, C. C. (2010). The relationship between employees' perception of emotional blackmail and their well-being. *Procedia Social and Behavioral Sciences 5,* 299-303.

Miceli, T. J. (2011). The real puzzle of blackmail: An informational approach. *Information Economics and Policy*, 23, 182-188.

Ramdinmawii, E., Ghisingh, S., & Sharma, U. M. (2014). A Study on the Cyber-Crime and Cyber Criminals: A Global Problem. *International Journal of Web Technology, 03,* June, 172-179.

Wolak, J., Finkelhor, D. (2016). *Sextortion: Keys findings from an online survey of 1,631 victims*. Durham: Crimes against children research centre, University of New Hampshire.

قدم في: أبريل 2018
أجيز في: فبراير 2019