الوعي المجتمعي بالجرائم المعلوماتية المرتبطة بالحياة الخاصة

إعداد

نهى فريد بكري

قسم علم الاجتماع والخدمة الاجتماعية

كلية الآداب والعلوم الإنسانية –جامعة الملك عبدالعزيز

ملخص البحث:

هدفت الدراسة إلى تحديد وعي مستخدمي مواقع التواصل الاجتماعي بمفهوم الجرائم المعلوماتية المرتبطة بالحياة الخاصة، وتصنيف أنواع الجرائم المعلوماتية المرتبطة بالحياة الخاصة، وتعد هذه الدراسة من الدراسات الوصفية التي تعمل على دراسة مشكلات أو ظواهر علمية وتحليلها وتفسيرها عبر المعلومات التي تم جمعها، وقد اعتمدت الدراسة على منهج المسح الاجتماعي بالعينة العمدية لتحقيق أهداف الدراسة وتساؤلاتها تمثلت عينة الدراسة في ٥٧٠ مشاركًا فردًا من المجتمع السعودي، ممن يُصنفون كمستخدمين لمواقع التواصل الاجتماعي فوق سن الثامنة عشرة، من خلال أداة الاستبانة؛ للوقوف على الوعي المجتمعي بالجرائم المعلوماتية المرتبطة بالحياة الخاصة.

وقد توصلت الدراسة إلى عدة نتائج مهمة منها: أن غالبية أفراد العينة لديهم مستويات عالية من الوعي حول مفهوم الجرائم المعلوماتية المرتبطة بالحياة الخاصة، حيث وافق 64.0 % على أن هذه الجرائم تشمل أي نشاط رقمي غير قانوني يهدف لتحقيق مكاسب مادية أو معنوية، كما توصلت الدراسة إلى أن غالبية أفراد العينة يوافقون بدرجة كبيرة على أن الجرائم المعلوماتية المتعلقة بالحياة الخاصة تمثل مشكلة خطيرة، خاصة في جرائم التحرش والابتزاز المعلوماتي، كما توصلت النتائج الى ان غالبية أفراد العينة يوافقون على أن تعريض الطفل للإهانة أو السخرية عبر حسابات البالغين يمثل تعديًا واضحًا، حيث وافق ٧٩.١% منهم على هذه العبارة، وتوصلت الدراسة إلى أن الجرائم المعلوماتية المتعلقة بانتهاك الخصوصية حظيت بتقييم مرتفع من قِبل أفراد العينة، حيث اعتُبر الابتزاز المعلوماتي أخطرها، إذ وافق على ذلك ٨٦.٠% من المشاركين. يليه التحرش المعلوماتي، الذي حصل على تأييد ٨٣.٠% من العينة.

وخرجت الدراسة بعدة توصيات من أهمها تكثيف الجهود التوعوية حول مخاطر الجرائم المعلوماتية المرتبطة بالحياة الخاصة، من خلال حملات إعلامية عمل تسلط الضوء على أساليب الوقاية منها. كما أكدت على ضرورة تعزيز القوانين والتشريعات لضمان حماية أقوى للخصوصية وفرض عقوبات رادعة على المخالفين. إضافةً إلى ذلك، شددت على أهمية تطوير آليات الإبلاغ والحماية الرقمية، من خلال إنشاء منصات سهلة الاستخدام تمكّن الأفراد من التبليغ بسرية وسرعة، وتعزيز وسائل الأمان الإلكتروني لضمان بيئة رقمية أكثر أمانًا.

الكلمات المفتاحية: الجرائم المعلوماتية، الحياة الخاصة، التنمر، الابتزاز، التحرش.

Abstract

This study aimed to identify the awareness of social media users regarding the concept of cybercrimes related to private life, as well as to classify their various forms. It is categorized as a descriptive study that seeks to examine, analyze, and interpret scientific problems or phenomena using collected data. To fulfill its objectives and address its research questions, the study adopted the social

survey method with a purposive sample. A total of 570 individuals from Saudi society participated, all of whom were social media users over the age of eighteen. Data collection was carried out using a questionnaire designed to assess public awareness of cybercrimes affecting private life.

Findings revealed that the majority of participants demonstrated a high level of awareness regarding the concept of cybercrimes related to private life. Notably, 64.0% agreed that these crimes include any illegal digital activity aimed at achieving material or moral benefits. A considerable portion of the sample also strongly agreed that such crimes pose a serious threat, especially in cases of digital harassment and blackmail. Additionally, 79.1% of respondents affirmed that exposing children to humiliation or ridicule through adult accounts on social media constitutes a clear violation.

Privacy-related cybercrimes were ranked among the most concerning issues, with electronic blackmail being identified as the most dangerous by 86.0% of participants, followed by online harassment, which received 83.0% agreement.

In conclusion, several key recommendations were proposed. Among them is the need to intensify awareness efforts about the dangers of cybercrimes related to private life through targeted media campaigns. The findings also highlight the necessity of reinforcing legal frameworks to ensure stronger privacy protection and to impose strict penalties on violators. Furthermore, enhancing digital safety mechanisms was emphasized, particularly through the development of user-friendly platforms that enable individuals to report incidents confidentially and efficiently, thereby fostering a more secure digital environment.

Keywords: Cybercrimes, Private Life, Bullying, Blackmail, Harassment**.**

مقدمة:

شهد العالم منذ الربع الأخير من القرن العشرين تحولات رقمية غير مسبوقة، حيث أصبحت التكنولوجيا الرقمية جزءًا لا يتجزأ من الحياة اليومية، مما أدى إلى إعادة تشكيل أنماط التفاعل

الاجتماعي والسلوك البشري. ومع انتشار الإنترنت وتطور وسائل التواصل الاجتماعي، أصبح الفضاء الرقمي بيئة أساسية للتواصل، التعلم، العمل، والتسوق، الأمر الذي أدى إلى توسع نطاق التعاملات الإلكترونية بين الأفراد والمؤسسات. غير أن هذا التطور الهائل رافقه تحديات أمنية واجتماعية معقدة، من أبرزها تصاعد الجرائم المعلوماتية، لا سيما تلك المرتبطة بالحياة الخاصة.

تعد الجرائم المعلوماتية المرتبطة بالحياة الخاصة من أخطر الظواهر الناشئة في العصر الرقمي، إذ تشمل العديد من الأشكال والممارسات التي تستهدف الأفراد بشكل مباشر، مثل التنمر المعلوماتي، التحرش الإلكتروني، الابتزاز الرقمي، اختراق البيانات الشخصية، والتجسس المعلوماتي. هذه الجرائم لم تعد مقتصرة على الأفراد العاديين فحسب، بل باتت تهدد المؤسسات والأسر، ما يجعلها مشكلة تتطلب اهتمامًا متزايدًا من الجهات المختصة والمجتمع ككل. وبسبب طبيعة الفضاء السيبراني الذي يتميز بعدم وجود حدود جغرافية، أصبح من الصعب تعقب مرتكبي هذه الجرائم، مما يستدعي تعزيز الوعي المجتمعي كأحد الحلول الأساسية لمواجهتها.

في ظل هذا السياق، يكتسب الوعي المجتمعي بالجرائم المعلوماتية المرتبطة بالحياة الخاصة أهمية كبيرة، حيث يمثل خط الدفاع الأول لحماية الأفراد والمجتمعات من الوقوع ضحية لهذه الجرائم. فكلما زادت معرفة الأفراد بمخاطر الفضاء الرقمي وأساليب الاحتيال الإلكتروني، كلما تمكنوا من اتخاذ التدابير الوقائية اللازمة لحماية بياناتهم الشخصية وحياتهم الخاصة. إضافة إلى ذلك، فإن التوعية الفعالة تساعد على تقليل حالات الاستغلال الرقمي، سواء من خلال الابتزاز أو التشهير أو الاختراقات غير القانونية.

في المملكة العربية السعودية، تشير الإحصائيات إلى أن أكثر من ٩٤% من السكان يستخدمون وسائل التواصل الاجتماعي، ما يجعل المجتمع السعودي واحدًا من أكثر المجتمعات تفاعلاً في الفضاء الرقمي. وبالرغم من تبني المملكة أنظمة وتشريعات صارمة لمكافحة الجرائم المعلوماتية، فإن استمرار ارتفاع معدلات هذه الجرائم يعكس وجود فجوة في الوعي المجتمعي حول طبيعتها، وآليات مواجهتها، وطرق الوقاية منها. فالعديد من الأفراد قد يكونون عرضة لهذه الجرائم بسبب ضعف إدراكهم للمخاطر المحتملة أو لعدم معرفتهم بالقوانين التي تحميهم والإجراءات القانونية المتاحة لهم في حال تعرضهم لأي نوع من الجرائم الإلكترونية.

تهدف هذه الدراسة إلى تحديد مستوى وعي مستخدمي مواقع التواصل الاجتماعي بمفهوم الجرائم المعلوماتية المرتبطة بالحياة الخاصة، بالإضافة إلى تصنيف أنواع هذه الجرائم. كما تسعى إلى تقديم فهم أعمق للواقع الحالي، مما يسهم في تطوير استراتيجيات فعالة للحد من الجرائم المعلوماتية التي تمس الحياة الخاصة وتعزيز سبل الحماية في الفضاء الرقمي. وتكمن أهمية الدراسة في تسليط الضوء على دور المؤسسات الرسمية في تعزيز الوعي المجتمعي بهذه الجرائم، من خلال حملات التوعية وبرامج التدريب والتشريعات الداعمة. كما تتناول الدراسة التحديات التي تواجه الأفراد في

التعرف على هذه الجرائم وطرق الوقاية منها، إضافةً إلى آليات الإبلاغ عنها. وتناقش الدراسة أيضًا تأثير الجرائم المعلوماتية على الحياة الخاصة للأفراد والمجتمع، وأهمية تضافر الجهود بين الجهات المعنية لحماية الخصوصية الرقمية. ومن خلال تحليل الواقع الحالي، تهدف الدراسة إلى تقديم توصيات تسهم في الحد من هذه الجرائم وخلق بيئة إلكترونية أكثر أمانًا. كما تسلط الضوء على أهمية التوعية الرقمية ودور الأفراد في التصدي لهذه التحديات، مع التركيز على تعزيز الثقافة القانونية المتعلقة بالجرائم المعلوماتية. وتبرز الدراسة أهمية التعاون بين المؤسسات الأمنية والقانونية والتعليمية لنشر الوعي حول سبل الحماية القانونية والرقمية. وبذلك، توفر الدراسة رؤية متكاملة تساعد في وضع حلول فعالة للحد من انتشار الجرائم المعلوماتية التي تهدد خصوصية الأفراد في الفضاء الرقمي.

مشكلة الدراسة:

أصبح تصاعد الجرائم المعلوماتية المرتبطة بالحياة الخاصة أحد التحديات الأمنية والاجتماعية في العصر الرقمي، حيث لم تعد هذه الجرائم مقتصرة على الدول النامية، بل تعاني منها حتى الدول المتقدمة، فقد أظهرت دراسة لمنظمة Symantec, 2019، أن 978 مليون شخص في ٢٠ دولة تعرضوا لجرائم إلكترونية خلال عام واحد، مع خسائر مالية تجاوزت 172 مليار دولار، أما في المملكة العربية السعودية، فقد شهدت معدلات الجرائم المعلوماتية ارتفاعًا ملحوظًا في السنوات الأخيرة، مواكبةً للاتجاهات العالمية، وتُشير تقارير وزارة العدل السعودية إلى أن المحاكم تعاملت مع 4,783 قضية جرائم معلوماتية في عام ٢٠٢٢، مما يمثل زيادة بنسبة ٥٥% مقارنة بعام ٢٠٢١، الذي سجل 2,723 قضية، كما ارتفع عدد الأفراد الذين تمت محاكمتهم بسبب جرائم الإنترنت بنسبة ٦٧% على أساس سنوي (لقمان، ٢٠٢٣)، ورغم التشريعات الصارمة التي أقرتها المملكة، فقد كشف تقرير حديث عن ارتفاع عدد المتهمين في قضايا الجرائم المعلوماتية بنسبة ٦٦.٨٨% في عام ٢٠٢٢ مقارنة بالعام السابق.

تعكس هذه الإحصائيات الارتفاع المستمر في الجرائم المعلوماتية المرتبطة بالحياة الخاصة، مما يستدعي النظر في طبيعة هذه الجرائم وآليات حدوثها في الفضاء السيبراني، وبما أن هذه الجرائم لا تقع بمعزل عن الاستخدام اليومي للتقنيات الرقمية، فإن فهم انتشارها يستوجب النظر إلى طبيعة البيئة الرقمية التي تشكل مسرحًا لها، ووفقًا لنظرية الأنشطة الروتينية، فإن حدوث الجريمة يرتبط بتوافر جاني محتمل، وضحية مناسبة، وغياب الحماية الكافية، وهو ما يظهر بوضوح في الفضاء السيبراني، حيث يُسهل انخفاض الوعي بالجرائم المعلوماتية واستغلال الثغرات الأمنية ارتكاب هذه الجرائم في بيئة تفتقر إلى الرقابة التقليدية، مما يجعلها أكثر تعقيدًا من حيث الكشف والمساءلة.

بناءً على ما سبق، تهدف الدراسة إلى التعرف على مستوى وعي المجتمع بالجرائم المعلوماتية المرتبطة بالحياة الخاصة، وذلك من خلال عدد من الأهداف الفرعية وهي كالتالي:

١. **تحديد وعي مستخدمي مواقع التواصل الاجتماعي بالجرائم المعلوماتية المرتبطة بالحياة الخاصة .**
٢. **تصنيف أنواع الجرائم المعلوماتية التي تمس الحياة الخاصة.**

وتبرز من خلال التساؤلات التالية:

١. ماهي محددات وعي مستخدمي مواقع التواصل الاجتماعي بالجرائم المعلوماتية المرتبطة بالحياة الخاصة؟
٢. ماهي أنواع الجرائم المعلوماتية المرتبطة بالحياة الخاصة؟

أهمية البحث:

تنبع أهمية هذه الدراسة من سعيها إلى تحديد وعي مستخدمي مواقع التواصل الاجتماعي بمفهوم الجرائم المعلوماتية المرتبطة بالحياة الخاصة، وهو ما يسهم في قياس مدى إدراك الأفراد للمخاطر الرقمية التي قد تهدد خصوصيتهم. كما تبرز أهمية الدراسة في تصنيف أنواع هذه الجرائم، مما يساعد في التعرف على أكثر التهديدات شيوعًا وتأثيرها على الأفراد والمجتمع. ومن خلال ذلك، توفر الدراسة قاعدة معرفية تسهم في تعزيز جهود التوعية، ودعم الجهات المختصة في وضع استراتيجيات أكثر فاعلية لحماية المستخدمين في البيئة الرقمية. بالإضافة إلى ذلك، تساعد نتائج الدراسة في تطوير سياسات وقائية وتشريعية تحد من انتشار الجرائم المعلوماتية التي تستهدف الحياة الخاصة، مما يسهم في خلق بيئة إلكترونية أكثر أمانًا واستقرارًا. وذلك على **النحو التالي:**

الأهمية العلمية

تبرز أهمية هذه الدراسة على المستوى العلمي من خلال النقاط التالية:

تتمثل الأهمية العلمية لهذه الدراسة في إثراء المعرفة الأكاديمية حول الجرائم المعلوماتية المرتبطة بالحياة الخاصة، من خلال تحليل مستوى وعي مستخدمي مواقع التواصل الاجتماعي بهذا النوع من الجرائم وتصنيف أنواعها المختلفة. كما تسهم الدراسة في سد الفجوة البحثية المتعلقة بفهم مدى إدراك الأفراد للمخاطر الرقمية وتأثيرها على الخصوصية. ومن خلال تقديم إطار نظري وتحليلي شامل، يمكن أن تكون هذه الدراسة مرجعًا علميًا يُستفاد منه في الدراسات المستقبلية حول

الأمن الرقمي وسبل الحماية من الجرائم المعلوماتية. علاوة على ذلك، تتيح نتائج الدراسة إمكانية تطوير نماذج وأساليب بحثية جديدة تسهم في تقييم وتحليل وعي الأفراد بالمخاطر السيبرانية، مما يدعم الجهود الأكاديمية في مجال الأمن الرقمي والجرائم المعلوماتية.

الأهمية العملية:

تتمثل الأهمية العملية لهذه الدراسة في دورها في تقديم معلومات قابلة للتطبيق تساعد في رفع مستوى وعي مستخدمي مواقع التواصل الاجتماعي بالجرائم المعلوماتية التي تمس الحياة الخاصة. فمن خلال تصنيف أنواع هذه الجرائم وتحليل مدى إدراك الأفراد لها، يمكن توجيه جهود التوعية بشكل أكثر فعالية، سواء من خلال الحملات الإعلامية أو البرامج التدريبية. كما تسهم الدراسة في مساعدة الجهات المعنية، مثل المؤسسات القانونية والأمنية، على تطوير سياسات وتشريعات تعزز الحماية الرقمية وتحد من انتشار الجرائم المعلوماتية. بالإضافة إلى ذلك، توفر نتائج الدراسة قاعدة بيانات يمكن أن تُستخدم في تصميم استراتيجيات أمنية أكثر كفاءة، مما يسهم في خلق بيئة إلكترونية أكثر أمانًا ويحد من المخاطر التي تهدد خصوصية الأفراد في الفضاء الرقمي.

حدود الدراسة

١. **المجال المكاني:** تم نشر الاستبانة إلكترونيًا عبر منصات التواصل الاجتماعي، مما أتاح مشاركة أفراد من مختلف مناطق المملكة العربية السعودية، ونظرًا لاعتماد التوزيع على الشبكات الاجتماعية للباحثة، فقد تكون هناك احتمالية لتركيز بعض الاستجابات في المناطق الأقرب جغرافيًا، ولكن لم يتم قياس ذلك بشكل مباشر ضمن أدوات الدراسة.
٢. **المجال البشري (عينة الدراسة):** مستخدمي مواقع التواصل الاجتماعي ممن فوق الثامنة عشرة، بلغ عدد المشاركين في الاستبانة 570 مشاركًا، متجاوزًا العدد المستهدف البالغ 500 مشارك، مما يعزز قوة العينة ويمكّن من تحليل أكثر دقة لمستوى الوعي المجتمعي بالجرائم المعلوماتية.
٣. **المجال الزمني:** جمع البيانات عبر الاستبانة الإلكترونية: بدأ في 27 - 31 أكتوبر ٢٠٢٥ وتم إيقافها لتجاوز العدد المطلوب.

الإطار النظري للدراسة:

أولاً: مفهوم الجرائم المعلوماتية:

١. جدلية المفهوم:

تعدّدت النماذج المعروضة لتعريف المصطلحات المستخدمة للدلالة على تلك الظاهرة الإجرامية الناشئة في بيئة الحاسوب وبيئة الشبكات، وهو تباين رافق مسيرة نشأة وتطور ظاهرة الإجرام المرتبط بتقنية المعلومات، وقد جاءت بعض المصطلحات ضيّقة لا تستوعب كافة النماذج الإجرامية، في حين جاء البعض الآخر فضفاضًا يصعب ضبطه وتحديد معالمه في ظل تطور الحاسوب وظهور "الإنترنت"، مما أضاف بُعدًا جديدًا لهذه الجرائم.

فمن مصطلح **إساءة استخدام الحاسوب** Computer abuse أو **جرائم الحاسوب** و**الجرائم المرتبطة بالحاسوب** Computer crimes - Computer related crimes، التي تشير جميعها إلى جرائم الحاسوب دون دلالة على دور "الإنترنت" في الجريمة، إلى **جرائم الإنترنت** Internet Crimes، الذي جاء مخالفًا للمصطلحات السابقة، حيث يشير إلى الجرائم التي تُرتكب عبر "الإنترنت"، لكنه قاصر عن احتواء بعض أشكال الجرائم المرتبطة بالحاسوب، مرورًا بمصطلح **الجريمة الإلكترونية** Electronic crimes، الذي يتسع ليشمل الفضاء "السيبراني" والوسائل التكنولوجية الأخرى إلى جانب الحاسوب، وهو أقرب المصطلحات لمفهوم **الجرائم المعلوماتية** Cyber crimes، الذي يتسع ليشمل الجرائم الواقعة على المعلومات والشبكات وتقنية المعلومات، ويُعتبر هذا المصطلح الأكثر شيوعًا واستخدامًا في الوثائق الدولية والدراسات الأجنبية الحديثة والمطبوعات الصادرة عن الأمم المتحدة، كما يتم استخدامه في المؤلفات القانونية والندوات والمؤتمرات الدولية والعربية.

إنّ عدم الاتفاق على استخدام **مصطلح موحد** للدلالة على الجرائم المعلوماتية، باعتبارها ظاهرة مستحدثة، أدّى بدوره إلى اختلاف وجهات النظر حول تقديم تعريف أو مدلول ثابت لها، بل إنّ بعض الباحثين امتنعوا عن تعريف الجرائم المعلوماتية بحجة أنّ هذا النوع من الإجرام ما هو إلا **جريمة تقليدية بأسلوب إلكتروني** (فتح الله، ٢٠١٩)، بالتالي يعتقدون أنّه من الخطأ اعتبار الجرائم المعلوماتية نوعًا خاصًا من الجرائم، بل يجب أن ينسحب عليها التعريف العام للجريمة، ويستندون في ذلك إلى أنّ الوسيلة المستخدمة في ارتكاب الجرائم المعلوماتية، سواء كانت شبكة "الإنترنت" أو الجهاز الإلكتروني، لا تغيّر شيئًا في طبيعة الجريمة أو أركانها العامة، إذ لا يقيم القانون وزنًا للوسائل أو الطرق التي تُرتكب بها الجرائم، فكما أنّه لا يوجد فرق بين من يستخدم يده أو أداة لنشل المارّة في قيام جريمة السرقة، فكذلك لا فرق بين من يستولي على حسابات الضحايا المصرفية بالاستيلاء المادي أو عبر الجهاز الإلكتروني، إذ تبقى الجريمة واحدة رغم اختلاف وسائل ارتكابها (عالية، ٢٠٢٠).

إلّا أنّ بعض العلماء اختاروا تعريف الجرائم المعلوماتية، رغم اتفاقهم على مبدأ تقليدية هذه الجريمة مع استخدامها لوسائل حديثة، ومن بينهم آرثر سولازر Arthur Solars، الذي اعتبر أنّ الجرائم المعلوماتية "نمط من أنماط الجرائم المعروفة في قانون العقوبات مرتبط بتقنية المعلومات"، وقد اتفق معه جوبتا (Gupta, 2014)، حيث يرى أنّ الجرائم

المعلوماتية "مصطلح يُستخدم لإدراج الجرائم التقليدية التي تُستخدم فيها الحواسيب أو الشبكات لتمكين الأنشطة غير القانونية"، ممّا يؤكد أنّ الحواسيب والشبكات ليست سوى وسائل للجريمة، وهو ما يتوافق مع رأي بانسال (Bansal, 2018)، التي ترى أنّ "الجرائم المعلوماتية هي أي جريمة جنائية تُستخدم فيها نظم تقنية المعلومات كوسيلة لارتكاب الجريمة".

إلّا أنّ رأياً ثالثاً لمجموعة باحثين استحسن تقسيم الجرائم المعلوماتية بناءً على معايير متنوعة، فمن المعيار القانوني تم تقسيم الجرائم المعلوماتية إلى تقليدية ومستحدثة حسب تقنينها ضمن قانون العقوبات أو أنّها لم تقنن بعد، في حين أنّ المعيار الاجتماعي قسّمها بحسب ألفة المجتمع لتلك الجرائم ومعرفته بها أو أنّه لم يعهدها من قبل.

وهنا يمكننا القول أنّ "غياب الإطار النظري المتسق في هذا الحقل من الجريمة.. إضافة لارتباط محاولات التعريف في أغلب الأحيان بمصطلحات كالافتراضية، الحاسوب، الإلكترونية، الرقمية، المعلوماتية.....وغيرها، عكس كثيراً من التداخل في المحتوى، كما عكس فجوات مهمة تعيق محاولات التعريف (Van der Hulst, 2008)، إلّا أنّ ذلك لم يثنِ العلماء والمختصين عن جهودهم المبذولة في محاولات تعريف الجرائم المعلوماتية، واستمروا بتقديم المزيد من التصنيفات لتسهيل تلك المهمة، فنجد من صنّفها إلى تعريفات الاتجاه الضيّق وتعريفات الاتجاه الواسع، والذي جاء أكثر وضوحاً في المراجع الأحدث بمسمى مختلف حيث صنفت الجرائم المعلوماتية إلى تعريفات المعايير المتعددة مقابل تعريفات المعيار المزدوج (المختلط)، يضاف للتصنيفين السابقين تصنيف التعريفات بحسب الحقول التخصصية التي تحاول تأطير الجرائم المعلوماتية استناداً على أسسها النظرية وتراكمها المعرفي، فنجد من يعرفها من الناحية الفنية، أو من الناحية القانونية، أو من الناحية الاجتماعية.

٢. الجرائم المعلوماتية في التشريعات العربية

لم يعرف كلاًّ من المشرّع اليمني في قانونه الصادر سنة ٢٠٠٦م، والمشرّع السوداني في قانون جرائم المعلوماتية ٢٠٠٧م، والمشرّع الجزائري ٢٠٠٩م، والمشرّع الأردني ضمن قانون جرائم أنظمة المعلومات ٢٠١٠م، وكذلك المشرّع الإماراتي متمثلًا في القانون الاتحادي بشأن مكافحة جرائم تقنية المعلومات ٢٠١٢م، والمشرّع البحريني ضمن جرائم تقنية المعلومات بمملكة البحرين ٢٠١٤م، والمشرّع المصري متمثلًا في قانون مكافحة جرائم تقنية المعلومات ٢٠١٨م الجرائم المعلوماتية تعريفًا محددًا.

بينما اتخذت التشريعات التالية موقفًا مغايرًا حيث عُرف التشريع السعودي ضمن نظام مكافحة الجرائم المعلوماتية في الفقرة ثمانية من المادة الأولى من نظام مكافحة جرائم

المعلوماتية السعودي ٢٠٠٧م، أنّ الجريمة المعلوماتية هي أي فعل يرتكب متضمنًا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام، كما عرف تشريع الجمهورية العربية السورية ضمن قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية ٢٠١٢م الجريمة المعلوماتية بأنها: "جريمة ترتكب باستخدام الأجهزة الحاسوبية أو تقع على المنظومات المعلوماتية أو الشبكة، وتنقسم الجرائم المعلوماتية أو (جرائم الفضاء السيبراني) إلى نوعين أساسيين: الأول هو الذي يكون فيه الحاسوب أو الشبكة مجرد وسيلة تسمح بارتكاب الجريمة وهي غالبًا جرائم اعتيادية، مثل: جريمة التهديد عن طريق الإنترنت، لكن الضرر منها عادةً ما يكون أعظم، والثاني هو الذي تكون فيه المنظومة المعلوماتية أو الشبكة موضوعا للجريمة، مثل: اختراق المنظومات المعلوماتية وتخريبها، وهي غالبًا جرائم مستحدثة لا بد من النص على أركانها ومعاقبتها".

يضاف إلى ذلك تعريف المشرّع القطري في قانون مكافحة الجرائم الإلكترونية ٢٠١٤م، حيث عرّف الجرائم المعلوماتية بأنها: "أي فعل ينطوي على استخدام وسيلة تقنية المعلومات أو نظام معلوماتي أو الشبكة المعلوماتية بطريقة غير مشروعة بما يخالف أحكام القانون"، وضمن ذات السياق عرّف المشرّع الكويتي ضمن قانون مكافحة جرائم تقنية المعلومات ٢٠١٥م الجرائم المعلوماتية بأنها: "كل فعل يرتكب من خلال استخدام الحاسب الآلي أو الشبكة المعلوماتية أو غير ذلك من وسائل تقنية المعلومات بالمخالفة لأحكام هذا القانون"، كما قام المشرع الليبي ضمن قانون مكافحة الجرائم الإلكترونية بتعريف الجرائم المعلوماتية ٢٠٢٢م بأنها: "كل فعل يرتكب خلال استخدام أنظمة الحاسب الآلي أو شبكة المعلومات الدولية أو غير ذلك من تقنية المعلومات بالمخالفة لأحكام هذا القانون".

ويتضح مما تقدّم بأنه لا يوجد اتفاق على اصطلاح محدّد يجمع الأفعال المرتكبة ضمن الجرائم المعلوماتية تحت عنوان واحد، بل هنالك مقاربات مختلفة لتناول الجريمة، ليست على المستوى الدولي فحسب بل على المستوى الإقليمي والمحلي حول ما يعتبر جريمة معلوماتية.

٣. الجرائم المعلوماتية من الجانب الاجتماعي

لم تقتصر الإشكالات التي تثيرها الجرائم المعلوماتية بالنسبة للقائمين على مكافحتها عند حد وضع التعريف من الامتناع عنه، تمتد الإشكالية إلى نطاق القوانين العقابية والجنائية التقليدية، والتي تقتصر على حماية الأشياء المادّية الملموسة، أمّا بالنسبة للأشياء المعنوية المرتبطة بها فلم تمتد إليها الحماية إلا حديثًا.

تؤكّد على ذلك تعريفات الجريمة الاجتماعية حيث تعتبر سلوكًا مغايرًا للأعراف الاجتماعية المتعارف عليها في المجتمع، وبمفهومها العام الجريمة هي تلك الأفعال التي تضر بالفردً، لذلك تصدّى لها المجتمع وسنّ القوانين الجنائية والمجتمعية معًا، وأوجب احترامها

والامتثال إليها (الجميلي، ٢٠٠١)، كما تشمل الجريمة بالمنظور الاجتماعي جميع أنماط السلوك المضادّة للمجتمع، والتي تضر بالمصلحة الاجتماعية، وتشمل مجموعة من الأفعال الإجرامية الخارجة عن القيم والمعايير الاجتماعية التي تخضع للعقاب (شتا، ١٩٨٧).

قياسًا على تعريف الجريمة اجتماعيًا يمكن أن ندرج هنا تعريف الجرائم المعلوماتية التي تركز على الضرر بالمجتمع وأفراده، ومن ذلك تعريفها بأنها: "القيام بالأنشطة التخريبية عمدًا أو التهديد بها عن طريق أجهزة الحاسوب وشبكة الإنترنت، وذلك بقصد إحداث ضرر، أو تحقيق أهداف اجتماعية أو فكرية أو سياسية أو غير ذلك، كما تعرف بأنها جميع أشكال السلوك غير المشروع أو الضار بالمجتمع والتي ترتكب باستخدام الحاسوب" (Pathore, 2016)، وعرفها (الخنين، ٢٠٠٨) بأنها: "نوع من الجرائم يكون مرتكبها ملمًّا بتقنيات وأنظمة الحاسوب والهواتف النقالة ويستخدم ما لديه من معرفة في تنفيذها بهدف تحقيق أغراض مشبوهة وأمور غير أخلاقية لا يرتضيها المجتمع لمنافاتها للأخلاق العامة"، هذا ويشير إليها (سعدات، ٢٠١٥) بأنها: "استخدام الأجهزة التقنية الحديثة، مثل: الحاسوب، أو الهاتف النقال، أو أحد ملحقاتها، أو برامجها في تنفيذ أفعالاً ذات أهدافًا تحمل مبادئًا وأفكارًا تتعارض مع التوجهات والأعراف الأخلاقية السائدة في المجتمع".

وقد عرفت الجرائم المعلوماتية في موضع آخر بأنها: "الجرائم التي ترتكب ضد الأفراد أو المجموعات من قبل أفراد ذوي دوافع إجرامية؛ بغرض إلحاق الضرر بصورة متعمدة بسمعة الضحية، أو إلحاق ضرر جسدي أو نفسي به، بشكل مباشر أو غير مباشر، وذلك باستخدام شبكات الاتصالات الحديثة على الإنترنت، مثل: غرف الدردشة والبريد الإلكتروني، والرسائل النصية على الهواتف النقالة، وقد أشار الجهني بأنها انفعالات سلوكية غير سوية بواسطة الأساليب والوسائل التقنية والإلكترونية ممّا يترتب عليه إلحاق أذى مادي أو معنوي للآخرين"، كما يرى (الغافري، ٢٠٠٩) بأنها: "جميع الأفعال غير المشروعة التي ترتكب بواسطة شبكة الإنترنت أو عبرها؛ بغرض الإضرار بحق أو مصلحة ما"، في حين عرفها (المقصودي، ٢٠١٥) بأنها: "كل استخدام في صورة فعل أو امتناع غير مشروع لتقنيات المعلومات بهدف الاعتداء على أي مصلحة مشروعة سواء كانت مادية أو معنوية".

كما أُشير إلى الجرائم المعلوماتية أيضا بأنها: "جميع الأنشطة التي تؤدي بغرض إجرامي في الفضاء المعلوماتي وتستهدف هذه الأنشطة ثلاث فئات للأشخاص والمنظمات التجارية وغير التجارية والحكومات" (القريني، ٢٠١٢)، وصوّرها (الشوابكة، ٢٠٠٩) بأنها: "كل عمل أو امتناع عن عمل يقوم به الفرد لإلحاق الضرر بالآخرين باستخدام مكونات الحاسوب المادية (أجهزة) والمعنوية (برامج وشبكات الاتصال)، وهذه الأعمال تعتبر إجرامية؛ لأن الوسائط المستخدمة لارتكابها تعتبر من المصالح والقيم والأصول التي تمتد القوانين الجنائية لحمايتها".

ثانياً: مفهوم الحياة الخاصة

أثارت فكرة الحق في الخصوصية جدلًا في القانون الوضعي، وقد أُستخدم مصطلح الخصوصية في القرن الخامس عشر في اللغة الإنجليزية، ويعني الحالة أو الوضع الذي يكون فيه الشخص بعيدًا عن مجتمع الآخرين أو الابتعاد عن محل اهتمام المحيطين به، إلّا أنّ نقطة الانطلاق نحو تطور الحق في الخصوصية بدأت في مقال شهير لكل من وارين وبراندیز (Brandeis & Warren, 1890).

إلّا أنّ العلماء لم يتفقوا على مفهوم موحد يتسم بالدقة لاصطلاح الحق في الحياة الخاصة؛ وفسّر بعض الباحثين السبب في ذلك لاتساع المفهوم وصعوبة تحديده، الأمر الذي حدا بالبعض إلى القول بأن مضمون هذا الحق "نسبي" أكثر منه "مطلق"، ونسبية مفهوم الحياة الخاصة للإنسان مفهوم يضيق ويتسع حسب ظروف وأحوال الشعوب الاقتصادية، والاجتماعية، والثقافية، وتأثرها بأعراف المجتمع وأخلاقياته، ومستواه الحضاري، فضلاً عن كون الفرد يعيش حياة مزدوجة عامة وخاصة، إلاّ أنّ القوانين تجمع على أن حرمة الحياة الخاصة تقتضي أن تظل مظاهرها بعيدة عن تدخل الغير وعن العلانية (الأهواني، ١٩٧٨).

لذلك تعددت تعريفات الحياة الخاصة والحق فيها، وتفاوتت في تحديد مضمون وطريقة رسم حدود هذا المفهوم، فقد رأى البعض (الحسيني، ١٩٩٥) أن هذا الحق يُعد "أحد الحقوق اللصيقة بالشخصية التي تثبت للإنسان لمجرد كونه إنسانًا"، كما يقررون أيضًا أنه من الصعوبة بمكان أن يتم عمل حصر للجوانب المتعددة لهذا الحق أو مفرداته، وذلك لصعوبة الحدود الفاصلة بين الحياة الخاصة والحياة العامة (عفيفي، ٢٠٠٣).

وفيما يخص التشريعات التي نصّت على الحق في الحياة الخاصة نجدها لم تضع تعريفًا محددًا له؛ ذلك لأن فكرة الحياة الخاصة من الأفكار المرنة التي ليس لها حدود ثابتة أو مستقرة؛ لذا نرى أن الفقه والقضاء في مختلف النظم القانونية ردّوها إلى اتجاهين، الأول: الاتجاه المعياري الذي يحاول أنصاره تحديد مدلول الحق في الحياة الخاصة استنادًا إلى معيار معين دون التطرق إلى بيان عناصره وتحديد حالاته، الثاني: والاتجاه التعددي الذي يحدد مفهوم هذا الحق عن طريق وضع قوائم بتعداد حالاته وتحديد عناصره المكونة له.

إلا أنه يمكن القول وبشكل عام أن معظم تلك المحاولات لم تخرج عن ثلاثة مذاهب وهي على النحو التالي: (السهلاني، ٢٠٢٠)، **المذهب الأول:** يرى أنصاره بأن الحياة الخاصة هي: "الحياة غير العامة التي تجري أحداثها ووقائعها خلف الجدران والأبواب المغلقة" (البهجي، ٢٠٠٥)، بهذا فالحياة الخاصة هي الحياة غير العلنية، أمّا الحياة العلنية فيقصد بها الحياة العامة، وبذلك يكون معيار التفرقة بين المفهومين هو المكان المغلق الذي تمارس فيه مظاهر الحياة الخاصة، بينما يرى أنصار **المذهب الثاني** أن الخصوصية تعني الوحدة فتوصف بأنها: "التحفظ وعدم تعريض الشخص

نفسه للجمهور دون موافقته ليتمتع بالسلم، وأن يترك وشأنه في أن يعتزل الناس" (عبد الرحمن، ١٩٩٦)، فتعرف الحياة الخاصة بأنها: "النطاق الذي يمكن للمرء في إطاره مكنة الانسحاب أو الانزواء عن الآخرين؛ بقصد تحقيق نوع من السكينة والحفاظ على سرية الحياة الخاصة"، في حين حاول أصحاب **المذهب الثالث** وضع تعريف للحياة الخاصة عن طريق بيان مظاهرها إلا أنهم اختلفوا في تحديد ما يعد من مظاهر الحياة الخاصة، وما لا يدخل في نطاقها، ومن هذه الآراء ما ورد في مؤتمر القانونيين لدول الشمال المنعقد في ستوكهولم ١٩٦٧م، بأن الاعتداء على الحق في الحياة الخاصة يكون بواسطة:

١. التدخل في حياتي الخاصة.
٢. التدخل في الكيان البدني والعقلي للإنسان.
٣. وضعه تحت الأضواء الكاذبة إذاعة وقائع تتصل بحياته الخاصة استعمار الاسم والصورة.
٤. التجسس والثلاثة الصوص والملاحظة.
٥. التدخل في سرية المراسلات.
٦. سوء استخدام الاتصالات.

بني على هذا المذهب تعريفات حديثة ذهبت للقول بأن الحياة الخاصة هي: "ذلك الجانب من حياة الإنسان التي يجب أن يترك فيه لذاته، ينعم بالألفة والسكينة بعيدًا عن نظر وسمع الآخرين وبمنأى عن تدخلهم أو رقابتهم دون مسوغ مشروع، وعرفت في موضع آخر بأنها: "حق المرء في أن يترك من أجل أن يعيش حياته الخاصة، وحمايته من التدخل في حياته الخاصة والعادية، أو التدخل في تكامله الجسماني والعقلي، أو الاعتداء على شرفه وسمعته، أو وضعه تحت أضواء خادعة، أو التجسس والمراقبة، أو الاستخدام السيئ الخاص باتصالاته الشخصية، أو استخدام المعلومات التي تؤخذ في حالات الثقة المهنية (فتوش، ٢٠٠٤).

مفهوم الجرائم المعلوماتية المتعلقة بالحياة الخاصة

تعددت مسميات الجرائم المعلوماتية التي تمارس ضمن شبكة الإنترنت أو من خلال مواقع التواصل الاجتماعي للاعتداء على الحياة الخاصة، حيث تستهدف تلك الجرائم تهديد حياة الأفراد، وفضح أسرارهم الشخصية، أو قذفهم والتشهير بهم بقصد الإضرار بسمعتهم، سواء كان ذلك بدافع الانتقام، أو تحقيق المنفعة المادية أو المعنوية من الضحية، أو لمجرد الفضول والتسلية.

ومن أبرز تلك المسميات مصطلح التنمر الإلكتروني Cyber Bullying، وعلى الرغم من أن التنمر في شكله التقليدي كان محصورًا في أفعال محددة، مثل الإيذاء المباشر جسديًا أو لفظيًا، أو السخرية والإهانة العلنية، إلا أنه في صيغته الرقمية اكتسب معاني أوسع وأكثر تعقيدًا. فقد توسعت المراجع في تعريفه ليشمل مجموعة متنوعة من الأفعال التي تُعد في حد ذاتها جرائم معلوماتية، لا سيما تلك المرتبطة بالحياة الخاصة، مثل: التهديد، والابتزاز، والتشهير، وانتحال

الشخصية، ونشر الأخبار المزيفة، والإزعاج، واقتحام الحياة الخاصة، واستغلال الأطفال جنسيًا، يُظهر هذا التوسع في المفهوم كيف أن الفضاء الافتراضي أضاف أبعادًا جديدة للتنمر، مما يجعله يتداخل مع أنماط متعددة من الجرائم المعلوماتية التي تمس الخصوصية بشكل مباشر".

إلّا أن الدراسة الحالية تفضل اصطلاح الجرائم المعلوماتية المتعلقة بالحياة الخاصة للدلالة على كلٍّ من الأفعال التالية: (التنمر المعلوماتي، التحرش المعلوماتي، الابتزاز المعلوماتي، استغلال الأطفال معلوماتياً)، والتي بلا شك تتضمن تعدٍ صارخ على حياة الأفراد الخاصة، ناهيك عن كونها ظواهر مستحدثة مخالفة للقانون، والانضباط، والاستقرار، حيث تعبر في مضمونها عن الانفلات وعدم الاكتراث بالضمير الجمعي للمجتمع.

إّن الواقع المعاش يتطلب مواجهة عصر جديد، بتحديات جديدة، وأخلاقيات مستحدثة، فرضتها تقنية جديدة، ممّا يستلزم معها إعادة النظر بشكل جدي في تحديد معارفنا وفق أسس وأخلاقيات متماشية مع مستجدات العالم الافتراضي الذي تكتنفه وأخلاق العالم التقليدي، إضافة إلى بعض الآداب والأخلاقيات التي فرضتها طبيعة هذا العالم الجديد، فالأخلاق واحدة إنما التغيير في مسرح الأحداث والأداة، بالتالي يكون لزاما علينا أن نحافظ على خصوصية الحياة الخاصة للفرد والأسرة وأن نحترم أمن وسرية المعلومات.

وقد اهتم المشرّع السعودي بحماية الحياة الخاصة وحرمتها، ضمن نظام مكافحة جرائم المعلوماتية ٢٠٠٧، فنجده يجرم الدخول غير المشروع لتهديد شخص أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعًا، ضمن المادة (٣) الفقرة (٢)، وفي المادة نفسها الفقرة (٤) يجرم النظام المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا أو ما في حكمها، وفي الفقرة (٥) يجرم النظام التشهير بالآخرين وإلحاق الضرر بهم عبر وسائل تقنيات المعلومات المختلفة، وتتراوح العقوبة بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على ٥٠٠,٠٠٠ أو بإحدى هاتين العقوبتين.

أما في المادة السادسة الفقرة (١) فقد أكد النظام على تجريم إنتاج ما من شأنه المساس بالنظام العام، أو القيم الدينية، أو الآداب العامة، أو حرمة الحياة الخاصة، أو إعداده، أو إرساله، أو تخزينه عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي، وحدد لذلك عقوبة السجن مدة لا تزيد على خمس سنوات وبغرامة لا تزيد على ٣,٠٠٠,٠٠٠ ريال أو بإحدى هاتين العقوبتين.

ومن منطلق اهتمام هذه الدراسة فيمكن أن تعرف الجرائم المعلوماتية المتعلقة بالحياة الخاصة بأنها " كل اعتداء يتضمن استخدام الحاسوب أو الشبكة المعلوماتية لارتكاب أيا من الأفعال التالية: (التنمر المعلوماتي، التحرش الجنسي المعلوماتي، الابتزاز المعلوماتي، استغلال الأطفال معلوماتياً).

ثانياً: أنواع الجرائم المعلوماتية المرتبطة بالحياة الخاصة:

١. **التنمر المعلوماتي:** عرّفه Patchin & Hinduja ٢٠١٥ بأنه "إلحاق الأذى المتعمد والمتكرر بالآخرين من خلال استخدام أجهزة الحاسوب، الهواتف المحمولة، وغيرها من الوسائط الرقمية"، وهو تعريف يُبرز الطبيعة المتعمدة والمستمرة لهذا السلوك، إضافة إلى تركيزه على الوسائل التكنولوجية المستخدمة في تنفيذه. ومن منظور أكثر شمولًا، يرى Agatston & Limber &Kowalski ٢٠١٤ أن التنمر المعلوماتي هو "أحد أشكال التنمر الذي يحدث عبر الأجهزة الرقمية مثل الهواتف المحمولة وأجهزة الحاسوب، ويتم من خلال الرسائل النصية، التطبيقات، الإنترنت، وخصوصًا عبر وسائل التواصل الاجتماعي، المنتديات، أو الألعاب الإلكترونية"، وهو تعريف يُضيء على السياقات الرقمية المتنوعة التي يُمارس فيها التنمر، مما يعكس تعقيد الظاهرة وتعدد أوجهها. وتؤكد هذه التعريفات أن التنمر الإلكتروني ليس فقط امتدادًا للتنمر التقليدي، بل هو ظاهرة قائمة بذاتها، تستلزم معالجة علمية وتشريعية خاصة، نظرًا لطبيعتها الخفية، وسهولة إعادة إنتاجها وانتشارها عبر المنصات الرقمية.

ويمكن التأكيد على أن التنمر المعلوماتي يحدث باستخدام التقنيات الرقمية، ويتم ذلك على وسائل التواصل الاجتماعي ومنصات المراسلة، ومنصات الألعاب، والهواتف المحمولة، ويتخذ عدة صور يمكن ذكر أهمها – حسب ما يتفق مع الدراسة - وذلك ما يلي:

- نشر أكاذيب، أو نشر صور، أو مقاطع فيديو محرجة لشخص ما على وسائل التواصل الاجتماعي.
- إرسال رسائل، أو صور أو مقاطع فيديو مؤذية أو مسيئة أو تهديدية عبر منصات المراسلة.
- انتحال شخصية شخص ما، وإرسال رسائل لئيمة إلى الآخرين نيابة عنهم، أو من خلال حسابات مزيفة (UNICEF, n.d.) .

٢. **التحرش المعلوماتي:** حسب لجنة الأمم المتحدة الاقتصادية والاجتماعية لغرب آسيا (الإسكوا)،يُشير المصطلح إلى أي سلوك غير مرغوب فيه ذي طابع جنسي يُمارس من خلال الوسائط الرقمية، مثل البريد الإلكتروني أو الرسائل النصية أو تطبيقات المحادثة وشبكات التواصل الاجتماعي، يُمكن لهذا النوع من التحرش أن يتخذ أشكالًا متعددة تشمل الرسائل الجنسية الصريحة، التهديد بالعنف الجنسي، أو استخدام لغة مهينة تستهدف هوية الضحية الجندرية أو خصائصها الشخصية مثل التوجه الجنسي أو الإعاقة. كما تُعرف الإسكوا التحرش الجنسي بأنه تلميحات جنسية هجومية أو متطفلة وغير مرغوب فيها قد تكون لفظية أو جسدية، وتحدث في السياقات العامة أو الخاصة. وبالتالي، فإن التحرش

الجنسي الإلكتروني يمثل امتدادًا رقميًا لسلوكيات قائمة، تعززها سهولة الوصول للضحايا عبر الوسائط الرقمية، وقد تتطلب أطرًا قانونية ومجتمعية خاصة لمواجهتها.

وقد عرف المشرع السعودي ضمن نظام مكافحة جريمة التحرش في المادة الأولى، بأن التحرش هو: "كل قول، أو فعل، أو إشارة ذات مدلول جنسي تصدر من شخص تجاه آخر تمس جسده، أو عرضه، أو تخدش حياءه بأي وسيلة كانت بما في ذلك وسائل التقنية الحديثة".

ويمكن أن تحدد أهم صور التحرش المعلوماتي كما يلي:

- إرسال كلمات أو تعليقات أو رموز مدلول جنسي.
- إرسال صور أو مقاطع ذات إيحاء أو مدلول جنسي.
- إرسال تسجيل صوتي أو التلفظ المباشر عبر الاتصالات المتضمنة في مواقع التواصل الاجتماعي ذات إيحاء أو مدلول جنسي.
- الطلب من الطرف الآخر الكشف عن أجزاء من جسدهـ/ـا بالصور أو الاتصالات المرئية عبر مواقع التواصل الاجتماعي.
- قيام شخص بأرسال صور أو فيديوهات له في أوضاع مخلة بالآداب.

٣. **الابتزاز المعلوماتي:** فعل يتضمن التهديد، والتهديد في مفهومه العام: "سلوك مادي ذو مضمون نفسي يتمثل في إنذار المهدد بإيقاع الأذى به هو شخصيًا، أو شخص عزيز لديه سواء كان إيقاع هذا الأذى مطلقًا من أي قيد أم مشروطًا بشرط، والتهديد ركن في الابتزاز المعلوماتي، ويراد به التلويح بإيقاع أذى لا ينصب على جسم المهدد، وإنّما يدخل الروع في نفسه، كالتهديد بحرق منزله، أو خطف ولده، أو إفشاء أمور ماسة بالشرف والاعتبار، سواء كانت متعلقة بالمجني عليه بشخص عزيز لديه، فيكون أخف على النفس استجابة مهدد إلى ما يطلبه الجاني" (بهنام، ١٩٩٩).

ويعرف الابتزاز بأنه "القيام بالتهديد بكشف معلومات معينة عن شخص أو فعل شيء؛ لتدمير الشخص المهدد إن لم يقم بالاستجابة إلى بعض الطلبات، وتكون هذه المعلومات محرجة عادة أو ذات طبيعة مدمرة اجتماعيًا"، وفي تعريف آخر هو: "محاولة الحصول على مكاسب معنوية أو مادية عن طريق الإكراه من شخص، أو أشخاص، أو حتى مؤسسات ويكون ذلك الإكراه بالتهديد بفضح سر من أسرار المبتز".

أما الابتزاز المعلوماتي فهو: "عملية تهديد وترهيب للضحية، بنشر صور أو مادة فيلمية، أو تسريب معلومات سرية، تخص الضحية مقابل دفع مبالغ مالية، أو استغلال الضحية للقيام بأعمال غير مشروعة" (صالح،٢٠٢١)، أو مشروعًا حسب المشرع السعودي طالما أنه كان مكرهًا.

ويتم عادة تصيّد الضحايا عن طريق البريد الإلكتروني، أو وسائل التواصل الاجتماعي المختلفة كمنصات: إكس X، انستغرامInstagram ، تيك توك TikTok، سناب شات Snapchat وغيرها من وسائل التواصل الاجتماعي؛ نظرًا لانتشارها الواسع واستخدامها الكبير من قبل جميع فئات المجتمع (لطفي، ٢٠١٨).

٤. **استغلال الأطفال معلوماتيًا:** ركزت معظم الأدبيات العربية والأجنبية التي تناولت استغلال الأطفال عبر الإنترنت بشكل أساسي على الجانب الجنسي، في حين أن هناك أشكالًا أخرى من الاستغلال لا تقل خطورة، مثل الاستغلال المعلوماتي للأطفال، الذي لم يحظَ باهتمام كافٍ في الأبحاث السابقة. ونظرًا لمحدودية هذا التركيز وبعده عن مجال الدراسة الحالية، برزت الحاجة إلى صياغة تعريف إجرائي يتناول بُعدًا آخر من استغلال الأطفال عبر الإنترنت، وهو الاستغلال المعلوماتي، والذي يمكن تعريفه بأنه "الممارسات التي يُستخدم فيها الأطفال كمحتوى أساسي في المنصات الرقمية ومواقع التواصل الاجتماعي بهدف زيادة المشاهدات والمتابعين، مما يؤدي إلى تحقيق أرباح مادية مباشرة من المنصات ذاتها، أو أرباح غير مباشرة من خلال جذب المعلنين أو الرعاة".

ويتجلى جوهر هذا الاستغلال في أن الطفل يُستخدم كوسيلة لتحقيق منفعة اقتصادية، وغالبًا ما يُمارس هذا النوع من الاستغلال من قبل أشخاص لهم ولاية أو سلطة أو مسؤولية على الطفل، مثل الوالدين أو الأقارب أو المعلمين، سواء كان ذلك بقصد تحقيق الأرباح أو بدون قصد، وفي كلتا الحالتين، يشكل ذلك انتهاكًا لحقوق الطفل وأحد أشكال الإساءة، وفق ما نص عليه المشرع السعودي في المادة الأولى من نظام حماية الطفل من الإيذاء، والتي تؤكد على أن كل ممارسة تُلحق ضررًا نفسيًا أو جسديًا أو اجتماعيًا بالطفل تُعد شكلًا من أشكال الإساءة.

يُعد الاستغلال المعلوماتي للأطفال أحد أشكال الإساءة، بناءً على المخاطر التي قد يتعرض لها الطفل نتيجة ظهوره في المحتوى الرقمي. فمن الناحية النفسية، قد يؤدي هذا الاستغلال إلى اضطرابات في الهوية وتقدير الذات، حيث يرتبط شعور الطفل بقيمته الشخصية بقدرته على جذب الانتباه أو تحقيق مكاسب تجارية، كما قد يواجه الطفل ضغطًا نفسيًا مستمرًا نتيجة التوقعات العالية للحفاظ على صورة أو سلوك معين أمام الجمهور، مما قد يؤدي إلى اضطرابات سلوكية طويلة الأمد. أما من الناحية الاجتماعية، فقد يعاني الطفل من العزلة الاجتماعية نتيجة نظرة المجتمع إليه كوسيلة لتحقيق الربح التجاري بدلًا من كونه فردًا مستقلًا. كما أن الانكشاف الرقمي الواسع يُعرِّض الطفل إلى انتهاك خصوصيته، حيث تصبح بياناته الشخصية وسلوكياته متاحة أمام الجمهور العام، مما قد يُؤثر على علاقاته الاجتماعية مستقبلًا.

تُعد مشاركة الأطفال في المحتوى الرقمي على نطاق واسع عاملاً يزيد من تعرضهم لمخاطر الجرائم المعلوماتية، مثل الابتزاز الإلكتروني أو الاستغلال من جهات غير موثوقة، مما يشكل تهديدًا مباشرًا لأمنهم وسلامتهم الشخصية. ونظرًا لهذه المخاطر، لا يقتصر الاستغلال المعلوماتي للأطفال عبر الإنترنت على كونه قضية اقتصادية، بل يمتد ليشمل أبعادًا نفسية، اجتماعية، حقوقية وقانونية، مما يستلزم توفير حماية شاملة لهم، ووفقًا لنظام حماية الطفل من الإيذاء ٢٠١٣[١]، تُعد إساءة معاملة الأطفال، سواء كانت جسدية، نفسية، اجتماعية أو معلوماتية، جريمة تستوجب التجريم والمعاقبة القانونية.

وعليه، فإن استخدام الأطفال كوسيلة لجذب المشاهدات والإعلانات على المنصات الرقمية، سواء كان ذلك من قِبل أولياء الأمور أو أي جهة تمتلك سلطة عليهم، يُعد مخالفة صريحة للأنظمة المعتمدة، لما ينطوي عليه من انتهاك لحقوق الطفل ومساس بسلامته النفسية والاجتماعية والجسدية. وهو ما يتوافق مع التشريعات السعودية الرامية إلى حماية حقوق الطفل في جميع البيئات، لا سيما البيئة الرقمية، التي باتت تتطلب المزيد من الرقابة والتشريعات الصارمة للحد من هذا النوع من الاستغلال.

إجراءات الدراسة وعرض النتائج

اولاً منهج الدراسة: تم استخدام المنهج الوصفي نظرًا لأن هذه الدراسة تنتمي إلى الدراسات الوصفية التحليلية التي تهدف إلى وصف الظاهرة وتحليل أبعادها.

ثانياً: مجتمع وعينة الدراسة: تكوّن مجتمع الدراسة من جميع الأفراد الذين تبلغ أعمارهم 18 عامًا فأكثر ممن يستخدمون مواقع التواصل الاجتماع، ونظرًا لضخامة حجم هذا المجتمع وتباين خصائص أفراده، تم استخدام العينة العمدية Purposive Sampling وهي أحد أنواع العينة غير العشوائية (غير الاحتمالية) Non – Probability Sample، والتي يتم اختيار المشاركين فيها بناءً على معايير محددة مسبقًا، بما ينسجم مع طبيعة الدراسة وأهدافها البحثية، حيث يعتمد الباحث على تحديد الأفراد الذين يمتلكون خصائص ذات صلة مباشرة بموضوع البحث، مما يعزز دقة النتائج وإمكانية تعميمها على الفئات المستهدفة المشابهة (Etikan *et al*, 2015). وبناءً على ذلك، تم اختيار ٥٧٠ مشاركًا وفق أسلوب العينة العمدية، الأمر الذي يتيح تحقيق تمثيل منهجي للفئة المستهدفة، ويوفر بيانات تتسم بالملاءمة والعمق التحليلي، مما يسهم في استخلاص استنتاجات قائمة على أسس علمية متينة (Palinkas *et al*. 2013).

[١] صدر نظام الحماية من الإيذاء بموجب المرسوم الملكي رقم م/٥٢ بتاريخ ١٥ ذو القعدة ١٤٣٤هـ -٢١ سبتمبر ٢٠١٣م

ثالثاً: الأساليب الإحصائية:

بناء على طبيعة الدراسة والأهداف التي سعت الباحثة إلى تحقيقها، تم تحليل بيانات الاستبيان باستخدام برنامج الحزمة الإحصائية للعلوم الاجتماعية SPSS v.27 واستخراج النتائج، وقد تم استخدام أساليب الإحصاء الوصفي التي تتمثل في التكرارات والنسب المئوية، للتعرف على خصائص أفراد عينة الدراسة وفقًا للبيانات الشخصية، والاجابة على تساؤلات الدراسة، وكذلك معامل ارتباط بيرسون ومعامل ثبات ألفا كرونباخ.

رابعاً: عرض نتائج الدراسة:

١) توزيع أفراد العينة حسب: النوع، العمر، الحالة الاجتماعية، الحالة التعليمية:

الجدول(١) الخصائص الديموغرافية لأفراد العينة

المتغير	التكرار	النسبة (%)
النوع		
ذكر	158	27.7
أنثى	412	72.3 *
المجموع	٥٧٠	١٠٠
العمر		
من 18 إلى أقل من23	154	27.0 *
من 23 إلى أقل من28	136	23.9
من 28 إلى أقل من33	72	12.6
من 33 إلى أقل من38	46	8.1
من 38 إلى أقل من43	51	8.9

من 43 فأكثر	111	19.5
المجموع	٥٧٠	١٠٠
الحالة التعليمية		
أقل من ثانوي	8	1.4
ثانوي	76	13.3
جامعي	401	* 70.4
دراسات عليا	81	14.2
أخرى	٤	0.7
المجموع	٥٧٠	١٠٠
الحالة العملية		
طالبـ/ـة	169	29.6
لا أعمل	154	* 27.0
موظفـ/ـة قطاع خاص	94	16.5
موظفـ/ـة قطاع حكومي	95	16.7
عمل خاص	58	10.2
المجموع	٥٧٠	%١٠٠
الحالة الاجتماعية		

أعزب/ عزباء	305	* 53.5
متزوج/ متزوجة	243	42.6
أرمل / أرملة	4	٠.7
مطلق / مطلقة	17	3.0
منفصلة	1	٠.2
المجموع	٥٧٠	١٠٠

***تشير إلى أعلى نسبة**

يلاحظ من الجدول (١) أن غالبية أفراد العينة من الإناث، حيث بلغت نسبتهن 72.3% مقارنةً بالذكور الذين يمثلون 27.7% فقط، ويشير هذا التفاوت إلى ميل العينة نحو العنصر النسائي والذي يمكن تفسيره من خلال توافقه مع ما أشارت إليه العديد من الدراسات التي تؤكد أن النساء غالبًا ما يكنّ أكثر إقبالًا على المشاركة في الاستبيانات مقارنة بالرجال، نظرًا لارتفاع مستوى الاهتمام بالتعبير عن الآراء والانخراط في الأبحاث الاجتماعية (Lindemann, 2019)

كما تتوزع العينة على عدة فئات عمرية، إلا أن النسبة الأكبر تتركز في الفئة العمرية من ١٨ إلى أقل من ٢٣ عامًا، والتي تمثل 27.0% من العينة، تليها الفئة من ٢٣ إلى أقل من ٢٨ عامًا بنسبة 23.9%، على الجانب الآخر، نجد أن الفئات العمرية المتوسطة تتوزع بشكل متوازن، حيث بلغت نسبة الفئة ٢٨ إلى أقل من ٣٣ عامًا 12.6%، في حين سجلت الفئة ٣٣ إلى أقل من ٣٨ عامًا 8.1%، والفئة ٣٨ إلى أقل من ٤٣ عامًا 8.9% يعكس هذا التوزيع مشاركة الأفراد في منتصف حياتهم المهنية والاجتماعية، الذين قد يكون لديهم خبرات حياتية مختلفة تؤثر على استجاباتهم مقارنة بالفئات الأصغر سنًا.

أما الفئات الأكبر سنًا، مثل من ٤٣ فأكثر، فتمثل 19.5%، وهو تمثيل جيد للفئات الأكبر سنًا، التي غالبًا ما تكون أقل مشاركة في الاستبيانات مقارنة بالفئات الأصغر، حيث تؤكد الدراسات أن الفئات العمرية المتقدمة قد تتردد أكثر في المشاركة في الأبحاث الإلكترونية أو الاستطلاعات عبر الإنترنت (Curtin, 2021)، مما يشير إلى تمثيل متوازن نسبيًا للعينة عبر مختلف الأعمار، يضمن شمولية النتائج وقدرتها على تقديم صورة دقيقة عن المجتمع المستهدف، كما يُسهم في إثراء الدراسة من خلال تقديم وجهات نظر متعددة تعكس اختلاف التجارب والخلفيات العمرية.

كما تظهر البيانات أن 70.4%من أفراد العينة حاصلون على مؤهل جامعي، مما يعني أن أغلب المشاركين لديهم مستوى تعليمي مرتفع، كما أن نسبة الحاصلين على دراسات عليا تصل إلى 14.2%، ما يشير إلى مشاركة جيدة من الأفراد الذين تابعوا تعليمهم بعد المرحلة الجامعية، في المقابل، تليها فئة الحاصلين على الثانوية بنسبة 13.3%، في حين سجلت فئة الحاصلين على دبلوم بنسبة 0.4%، وأخيراً سجلت فئة أقل من ثانوي نسبة منخفضة بلغت ١.٥٧.

وعند النظر إلى الحالة العملية، نجد أن النسبة الأكبر من العينة هم طلاب وطالبات، حيث بلغت نسبتهم 29.6%، يليهم الأفراد الذين لا يعملون بنسبة 27.0%، هذه النسب تعكس وجود عدد كبير من الشباب في العينة، وهو ما يتماشى مع الفئات العمرية الممثلة في الجدول، أما الموظفون، سواء في القطاع الحكومي أو الخاص، فيشكلون نسبة متقاربة، حيث بلغت 16.7% و١٦.٥% على التوالي. ومن الملاحظ أن نسبة الأفراد الذين يعملون في مشاريع خاصة هي الأقل، إذ لم تتجاوز 10.2%.

أما بالنسبة للحالة الاجتماعية، فتشير البيانات إلى أن أكثر من نصف العينة غير متزوجين بنسبة 53.5%، وهو ما يتماشى مع الفئات العمرية الشابة الممثلة في الدراسة، في المقابل، بلغت نسبة المتزوجين 42.6%، أما الفئات الأخرى مثل الأرامل والمطلقين، فتمثل نسبًا صغيرة جدًا، حيث لم تتجاوز 0.7% و٣.٠% على التوالي، بينما كانت نسبة المنفصلين 0.2% فقط.

بشكل عام، تعكس الخصائص الديموغرافية للعينة ميلها نحو الفئات الشابة والمتعلمة، مع تمثيل أكبر للإناث. كما يظهر أن معظم المشاركين هم طلاب أو غير عاملين، مما قد يؤثر على طبيعة النتائج المستخلصة من الدراسة، بالإضافة إلى ذلك، فإن الغالبية العظمى غير متزوجين، مما قد يكون له دلالات فيما يتعلق بموضوع البحث، هذه العوامل مجتمعة توضح طبيعة العينة وتساعد في فهم مدى تمثيلها للظاهرة المدروسة.

ثانيا: **عرض نتائج السؤال الأول حول "الوعي بالجرائم المعلوماتي المرتبطة بالحياة الخاصة"**

وتم قياسه من خلال ثلاثة أبعاد، هي: تعريفات الجرائم المعلوماتية، تعريفات الحياة الخاصة والجرائم المعلوماتية التي تعتبر تعدي على الحياة الخاصة، وقد تم حساب المتوسطات الحسابية والانحرافات المعيارية والترتيب لعبارات بعد تعريفات الجرائم المعلوماتية، وجاءت النتائج كما هو موضح في الجدول التالي:

الجدول (٢) المحور الأول: ماهية الجرائم المعلوماتي المرتبطة بالحياة الخاصة

البعد	العبارة	أوافق	محايد	لا	المتوسط	الانحراف	درجة	الرتبة

		ك(%)	ك(%)	أوافق ك(%)	الحسابي	المعياري	الموافقة	
البعد الاول: تعريفات الجرائم المعلوماتية	أي نشاط يستخدم التكنولوجيا الرقمية بشكل غير قانوني لتحقيق مكاسب مادية أو معنوية	(64.0) 365	(23.5) 134	(12.5) 71	2.52	0.71	أوافق	٩
	الجرائم التي تتضمن نشر صور أو بيانات خاصة دون إذن ويمكن أن تستخدم لابتزاز الأفراد أو إيذائهم نفسياً	(82.8) 472	(9.3) 53	(7.9) 45	2.75	0.59	أوافق	٣
	جرائم تتم باستخدام الحاسوب أو الإنترنت تشمل أفعال خارجة عن المعايير الاجتماعية	(69.5) 396	(21.6) 123	(8.9) 51	2.61	0.65	أوافق	٧
البعد الثاني: تعريفات الحياة الخاصة	حق الفرد في أن يترك وحده لا يعكر عليه أحد صفو خلوته	(59.1) 337	(28.8) 164	(12.1) 69	2.47	0.70	أوافق	١٠
	حق الفرد في الحفاظ على سرية حياته الأسرية والشخصية	(90.2) 514	(7.5) 43	(2.3) 13	2.88	0.39	أوافق	١
	الحفاظ على كل ما يؤدي إلى معرفة الفرد على وجه التحديد، أو يجعل التعرف عليه ممكنًا بصفة مباشرة أو غير مباشرة	(62.6) 357	(28.9) 165	(8.4) 48	2.54	0.65	أوافق	٨
البعد الثالث: الجرائم المعلوماتية التي تعتبر	التنمر المعلوماتي (الالكتروني) مثل المضايقة أو الإساءة إلى شخص آخر عن طريق التكنولوجيا الرقمية	(77.5) 442	(14.2) 81	(8.2) 47	2.69	0.62	أوافق	٥
	الابتزاز المعلوماتي(الالكتروني) تهديد للنشر أو كشف معلومات خاصة أو	(86.0) 490	(8.4) 48	(5.6) 32	2.80	0.52	أوافق	٢

تعدي على الحياة الخاصة	حساسة عن شخص ما إذا لم يتم تلبية مطالب معينة							
	التحرش المعلوماتي (الالكتروني) أقوال أو أفعال ذات مدلول جنسي تمس الجسد أو العرض أو تخدش الحياء	(83.0) 473	(8.9) 51	(8.1) 46	2.75	0.59	**أوافق**	٤
	استغلال الأطفال لتحقيق مكاسب مادية من خلال مواقع التواصل الاجتماعي "إعجابات أو إعلانات ...الخ"	(77.9) 444	(12.5) 71	(9.6) 55	2.68	0.64	**أوافق**	٦
المتوسط الكلي للمحور					**2.67**	**0.13**	**أوافق**	

يلاحظ من الجدول (٢) مستويات عالية من الوعي بين أفراد العينة حول مفهوم الجرائم المعلوماتية المرتبطة بالحياة الخاصة، حيث اتفق غالبية المشاركين على مختلف الأبعاد المتعلقة بتعريف هذه الجرائم وانتهاكات الخصوصية التي قد تحدث عبر الإنترنت، يعكس ذلك المتوسط الحسابي الكلي للمحور الذي بلغ ٢.٦٧ والانحراف المعياري ٠.١٣ إجماعًا قويًا على خطورة هذه الجرائم وأثرها السلبي على الأفراد.

كما يُلاحظ أن المشاركين لديهم فهم واسع لمفهوم الجرائم المعلوماتية، حيث وافق 64.0 % على أن هذه الجرائم تشمل أي نشاط رقمي غير قانوني يهدف لتحقيق مكاسب مادية أو معنوية، وهو ما يعكس وعيًا بأن الجرائم المعلوماتية لا تقتصر فقط على الاختراقات التقنية، بل تشمل أيضًا التنمر والابتزاز وغيرها من الجرائم التي تستهدف الإضرار بالأفراد نفسيًا واجتماعيًا، كما وافق 69.5% على أن الجرائم المعلوماتية تتضمن أفعالًا خارجة عن المعايير الاجتماعية باستخدام الحاسوب أو الإنترنت، مما يشير إلى إدراك بأن بعض السلوكيات الرقمية، حتى لو لم تكن ذات طابع مالي، قد تشكل جرائم يعاقب عليها القانون، أما الجريمة الأكثر وضوحًا بالنسبة للمشاركين، فهي نشر صور أو بيانات خاصة بدون إذن بهدف الابتزاز أو الإيذاء النفسي، حيث أيد ذلك 82.8%، بمتوسط حسابي مرتفع ٢.٧٥ وانحراف معياري منخفض ٠.٥٩، مما يدل على إجماع كبير على خطورة هذا السلوك باعتباره أحد أشد أنواع الجرائم المعلوماتية تأثيرًا على الحياة الخاصة.

كما أظهر أفراد العينة مستويات عالية من الوعي بمفهوم الحياة الخاصة، حيث اتفق غالبية المشاركين على مختلف الأبعاد المرتبطة به، مما يعكس إدراكًا واسعًا لأهمية الخصوصية وحمايتها

في السياقات الرقمية والاجتماعية. ويؤكد ذلك المتوسط الحسابي الكلي للمحور البالغ ٢.٧٠ والانحراف المعياري 0.40، مما يشير إلى إجماع كبير على مركزية الحياة الخاصة وضرورة حمايتها.

لوحظ أيضاً من النتائج أن حق الفرد في الحفاظ على سرية حياته الأسرية والشخصية حظي بأعلى مستوى من الأهمية لدى المشاركين، حيث بلغ المتوسط الحسابي 2.88 بانحراف معياري 0.39، مما يعكس وعيًا عالياً بأهمية السرية والخصوصية باعتبارها جوهر الحياة الخاصة، في المقابل، جاءت أهمية حق الفرد في أن يُترك وحده دون إزعاج خلال خلوته في المرتبة الأخيرة بمتوسط حسابي 2.47 وانحراف معياري 0.70، وبرغم تأخر هذه العبارة، إلا أن مستواها لا يزال مرتفعًا، مما يشير إلى أن أفراد العينة يعتبرون العزلة الطوعية جزءًا من مفهوم الحياة الخاصة، ولكن بدرجة أقل مقارنة بجوانب الخصوصية الأسرية والشخصية، ويُحتمل أن يكون ذلك نتيجة لاعتبارات ثقافية واجتماعية تحدد أولويات مفهوم الحياة الخاصة، حيث قد يُنظر إلى الخصوصية الأسرية والشخصية على أنها أكثر أهمية في السياقات الاجتماعية المحافظة، مقارنةً بالعزلة الشخصية.

وقد حظيت الجرائم المعلوماتية التي تعتبر تعديًا على الحياة الخاصة قد حصل على تقييم مرتفع من قِبل أفراد العينة، حيث بلغ متوسط الاستجابة ٢.٧٣ بانحراف معياري قدره ٠.٤٩، مما يعكس رفضًا واسعًا لهذه الجرائم وإدراكًا كبيرًا لخطورتها وتأثيرها المباشر على الأفراد، حيث اعتُبر الابتزاز الإلكتروني أخطر هذه الجرائم، إذ وافق على ذلك 86.0% من العينة، بمتوسط حسابي 2.80 وانحراف معياري 0.52، مما يدل على أن المشاركين يعتبرونه تهديدًا مباشرًا ومؤثرًا على الأفراد، كما جاء التحرش الإلكتروني في المرتبة الثانية، حيث أيده 83.0% من المشاركين، بمتوسط حسابي 2.75، مما يعكس خطورة استغلال الفضاء الافتراضي في الإيذاء النفسي والجسدي للأفراد، وهو ما ينطبق على التنمر المعلوماتي والذي وافق 77.5 % على أنه يُعد جريمة معلوماتية، بمتوسط حسابي بلغ 2.69، وأخيراً جاءت الجريمة المتعلقة باستغلال الأطفال لتحقيق مكاسب مادية من خلال مواقع التواصل الاجتماعي مثل الإعلانات أو المحتوى الرقمي بنسبة موافقة بلغت ٧٧.٩%، بمتوسط حسابي ٢.٦٨ وانحراف معياري ٠.٦٤، ورغم تأخرها في الترتيب، إلا أن مستواها المرتفع يعكس وعي المشاركين بمخاطر الاستغلال الرقمي للأطفال. ومع ذلك، قد تُعتبر أقل شيوعًا أو تأثيرًا مباشرًا مقارنة ببقية الأنواع التي تشكل تهديدًا فوريًا، بينما يتطلب استغلال الأطفال معالجة قانونية واجتماعية أعمق لحماية الفئات الأكثر ضعفًا.

بشكل عام، تشير هذه النتائج إلى أن المشاركين لديهم وعي مرتفع بمخاطر الجرائم المعلوماتية وتأثيرها على الحياة الخاصة، حيث أظهرت جميع العبارات مستوى موافقة مرتفع، يُعتبر التنمر والابتزاز والتحرش المعلوماتي من أخطر الجرائم وفقًا للمشاركين، مما يستدعي تعزيز القوانين الرادعة لهذه الممارسات، وزيادة التوعية الرقمية حول أساليب الحماية من هذه التهديدات. كما

تؤكد النتائج أهمية نشر ثقافة احترام الخصوصية، سواء من خلال توعية الأفراد بأهمية حماية بياناتهم الشخصية، أو من خلال تشديد الرقابة على الجهات التي تجمع وتستخدم هذه البيانات.

١. عرض نتائج السؤال الثاني حول "أنواع الجرائم المعلوماتية المرتبطة بالحياة الخاصة"

الجدول (٣) أنواع الجرائم المعلوماتية المرتبطة بالحياة الخاصة

البعد	العبارة	أوافق	محايد	لا أوافق	المتوسط الحسابي	الانحراف المعياري	درجة الموافقة	الرتبة
		ك(%)	ك(%)	ك(%)				
البعد الاول: أفعال التنمر المعلوماتي التي تعتبر تعدياً على الحياة الخاصة	نشر الشائعات عن شخص بهدف تشويه سمعته عبر مواقع التواصل الاجتماعي	(78.8) 449	(9.3) 53	(11.9) 68	2.67	0.68	أوافق	١٤
	فضح أسرار شخص عبر مواقع التواصل الاجتماعي	(78.1) 445	(8.8) 50	(13.2) 75	2.65	0.70	أوافق	١٦
	نشر صور أو مقاطع فيديو محرجة لشخص على مواقع التواصل الاجتماعي	(81.2) 463	(7.0) 40	(11.8) 67	2.69	0.67	أوافق	١٠
	إرسال رسائل أو صور أو مقاطع فيديو مؤذية أو مسيئة أو تهديدية لشخص عبر مواقع التواصل الاجتماعي	(79.3) 452	(7.7) 44	(13.0) 74	2.66	0.70	أوافق	١٥
	انتحال شخصية شخص وإرسال رسائل مسيئة أو	(76.1)	(9.5)	(14.4)	2.62	0.72	أوافق	١٧

	مزعجة إلى الآخرين نيابة عنه تجعله في ورطة	434	54	82				
	استثناء عمدا من جماعة على الإنترنت من قبل مشرف/ة المجموعة	(38.9) 222	(30.9) 176	(30.2) 172	2.09	0.83	**محايد**	٢٦
	الاستهزاء أو السخرية	(72.5) 413	(13.5) 77	(14.0) 80	2.58	0.72	**أوافق**	١٩
	التحقير بإرسال عبارات مهينة أو مؤذية غير حقيقية أو ظالمة عن شخص	(79.5) 453	(9.5) 54	(11.1) 63	2.68	0.66	**أوافق**	١٢
البعد الثاني: أفعال التحرش المعلوماتي التي تعتبر تعدياً على الحياة الخاصة	إرسال كلمات أو تعليقات أو رموز مدلول جنسي	(82.5) 470	(7.4) 42	(10.2) 58	2.72	0.64	**أوافق**	٥
	أرسال صور أو مقاطع ذات إيحاء أو مدلول جنسي	(83.3) 475	(6.7) 38	(10.0) 57	2.73	0.63	**أوافق**	١
	إرسال تسجيل صوتي أو التلفظ المباشر عبر الاتصالات المتضمنة في مواقع التواصل الاجتماعي ذات إيحاء أو مدلول جنسي	(81.8) 466	(7.7) 44	(10.5) 60	2.71	0.65	**أوافق**	٨
	الطلب من الآخر الكشف عن أجزاء من جسده/ا بالصور أو الاتصالات المرئية عبر مواقع التواصل	(81.9) 467	(7.9) 45	(10.2) 58	2.72	0.64	**أوافق**	٦

	الاجتماعي							
	قيام شخص بأرسال صور أو فيديوهات له في أوضاع مخلة بالآداب	(82.6) 471	(7.0) 40	(10.4) 59	2.72	0.64	**أوافق**	**٧**
البعد الثالث: أفعال الابتزاز المعلوماتي التي تعتبر تعديا على الحياة الخاصة	سرقة كلمات السر (المرور) أو بيانات الحاسب الخاصة بشخص مقابل مكاسب معنوية أو مادية	(80.9) 461	(8.8) 50	(10.4) 59	2.71	0.65	**أوافق**	**٩**
	التهديد عبر منصات التواصل الاجتماعي بنشر معلومات أو صور أو مقاطع تخص شخص آخر مقابل مكاسب معنوية أو مادية	(82.1) 468	(7.9) 45	(10.0) 57	2.72	0.63	**أوافق**	**٣**
	التهديد عبر وسائل التواصل الاجتماعي بنشر معلومات أو صور أو مقاطع تخص الضحية لإلحاق الضرر أو الانتقام	(82.8) 472	(7.2) 41	(10.0) 57	2.73	0.63	**أوافق**	**٢**
	التهديد بنشر معلومات أو صور أو مقاطع تخص شخص آخر لحملها/ا على فعل غير مشروع أو مشروع متضمنا ذلك إكراها	(82.5) 470	(7.5) 43	(10.0) 57	2.72	0.63	**أوافق**	**٤**
	الملاحقة عبر وسائل التقنية stalking	(69.1) 394	(17.9) 102	(13.0) 74	2.56	0.71	**أوافق**	**٢٠**

البعد الرابع: أفعال تعد استغلالاً لحياة الأطفال دون (١٨) الخاصة عبر مواقع التواصل الاجتماعي	إظهار يوميات الأطفال (الأكل، الاستيقاظ من النوم...الخ) ضمن حسابات الوالدين أو الأخوة	(15.1) 86	(24.7) 141	(60.2) 343	2.45	0.74	**أوافق**	**٢٤**
	تعريض الأطفال لمواقف اجتماعية مفتعلة لقياس ردة فعله أو مشاعره	(11.4) 65	(17.5) 100	(71.1) 405	2.60	0.69	**أوافق**	**١٨**
	إظهار الأطفال ضمن حسابات البالغين (معلمين، أقارب، جيران...الخ(	(17.9) 102	(25.8) 147	(56.3) 321	2.38	0.77	**أوافق**	**٢٥**
	تعريض الطفل للإهانة أو السخرية ضمن حسابات (الوالدين، الأخوة) في مواقع التواصل الاجتماعي	(10.7) 61	(9.5) 54	(79.8) 455	2.69	0.65	**أوافق**	**١١**
	تعريض الطفل للإهانة أو السخرية ضمن حسابات البالغين (معلمين، أقارب، جيران...الخ) في مواقع التواصل الاجتماعي	(11.2) 64	(9.6) 55	(79.1) 451	2.68	0.67	**أوافق**	**١٣**
	الحصول من خلال الطفل على الإعلانات التجارية (أي أن الطفل هو السبب الأساسي لاختيار الحساب للإعلان(	(14.2) 81	(21.2) 121	(64.6) 368	2.50	0.73	**أوافق**	**٢٣**

	إظهار الطفل بمواقف أو مظاهر أكبر من سنه، من خلال لبسه، أو سلوكياته، أو حواراته	(15.3) 87	(17.0) 97	(67.7) 386	2.52	0.75	أوافق	٢٢
	الحصول من خلال الطفل على عدد أكبر من المتابعين، والإعجابات	(13.0) 74	(19.5) 111	(67.5) 385	2.55	0.71	أوافق	٢١
المتوسط الكلي للمحور					٦٢٢.	٤٥.1	أوافق	

يلاحظ من الجدول (٣) أن جميع الأفعال المدرجة تحت مختلف الأبعاد المتعلقة بالجرائم المعلوماتية المرتبطة بالحياة الخاصة قد حصلت على درجة موافقة مرتفعة بشكل عام، حيث بلغ المتوسط الكلي للمحور ٢.٦٢ مع انحراف معياري قدره ٠.١٤، مما يشير إلى وجود إجماع واسع بين المشاركين على اعتبار هذه الأفعال تعديًا على الحياة الخاصة.

ففيما يخص البعد الأول، الذي يتعلق بأفعال التنمر المعلوماتي، فقد حصلت أغلب العبارات على درجة موافقة مرتفعة. على سبيل المثال، كان نشر الشائعات لتشويه السمعة عبر مواقع التواصل الاجتماعي من أكثر الأفعال التي وافق عليها المشاركون بنسبة ٧٨.٨%، بمتوسط حسابي بلغ ٢.٦٧ وانحراف معياري قدره ٠.٦٨. كما جاءت أفعال مثل نشر صور أو مقاطع فيديو محرجة لشخص وإرسال رسائل مسيئة أو تهديدية بنسبة موافقة بلغت ٨١.٢% و٧٩.٣% على التوالي، مما يعكس وعيًا كبيرًا بخطورة هذه الأفعال. بالمقابل، كانت درجة الموافقة أقل في بعض الأفعال مثل الاستثناء المتعمد من الجماعات عبر الإنترنت، حيث حصل هذا الفعل على أدنى درجة موافقة بنسبة ٣٨.٩% فقط، وكان المتوسط الحسابي له ٢.٠٩ مع انحراف معياري مرتفع نسبيًا بلغ ٠.٨٣، ما يشير إلى تباين وجهات النظر حوله.

أما بالنسبة للبعد الثاني، الذي يتناول أفعال التحرش المعلوماتي، فقد سجلت العبارات المتعلقة بإرسال محتوى جنسي أعلى نسب الموافقة بين جميع الأبعاد، حيث حصلت عبارة إرسال صور أو مقاطع ذات إيحاء جنسي على أعلى درجة موافقة بنسبة ٨٣.٣%، بمتوسط حسابي ٢.٧٣ وانحراف معياري ٠.٦٣، مما يبرز مدى إدراك المشاركين لخطورة هذا الفعل. كما جاءت أفعال أخرى مثل إرسال تسجيلات صوتية أو الطلب من الآخرين الكشف عن أجزاء من أجسادهم بنسب موافقة تتجاوز ٨١%، وهو ما يعكس إجماعًا واضحًا على اعتبار هذه الأفعال تعديًا صارخًا على الخصوصية.

فيما يخص البعد الثالث، المتعلق بأفعال الابتزاز المعلوماتي، فقد حصلت العبارات الواردة ضمن هذا البعد على نسب موافقة مرتفعة جدًا، إذ وافق ٨٢.٨% من المشاركين على أن التهديد بنشر معلومات أو صور بغرض الإضرار بالضحية يمثل تعديًا على الحياة الخاصة، بمتوسط حسابي ٢.٧٣ وانحراف معياري ٠.٦٣، مما يجعله من أكثر الأفعال اتفاقًا عليه. كما كانت هناك موافقة كبيرة على سرقة بيانات الحسابات الشخصية مقابل مكاسب، بنسبة ٨٠.٩%، مما يشير إلى خطورة هذه الظاهرة واعتبارها جريمة معلوماتية واضحة.

أما البعد الرابع، الذي يتناول استغلال حياة الأطفال عبر مواقع التواصل الاجتماعي، فقد حصلت العبارات الواردة فيه على درجات موافقة متفاوتة، حيث كانت بعض الأفعال أكثر رفضًا من غيرها. على سبيل المثال، حصلت عبارة إظهار يوميات الأطفال ضمن حسابات الوالدين على أقل نسبة موافقة بلغت ١٥.١% فقط، مع متوسط حسابي ٢.٤٥، مما يدل على أن المشاركين لا يعتبرون هذا الفعل تعديًا على الحياة الخاصة بنفس درجة الأفعال الأخرى. في المقابل، كانت هناك موافقة مرتفعة على أن تعريض الطفل للإهانة أو السخرية عبر حسابات البالغين يمثل تعديًا واضحًا، حيث وافق ٧٩.١% من المشاركين على ذلك، بمتوسط حسابي ٢.٦٨، ما يعكس حساسية هذا الموضوع لدى الجمهور.

بصورة عامة، يتضح من النتائج أن المشاركين متفقون بدرجة كبيرة على أن الجرائم المعلوماتية المتعلقة بالحياة الخاصة تمثل مشكلة خطيرة، خاصة في مجالات التحرش المعلوماتي والابتزاز المعلوماتي، حيث حظيت هذه الأفعال بأعلى درجات الموافقة. أما فيما يخص استغلال الأطفال، فقد تباينت وجهات النظر حول بعض الممارسات، مما يشير إلى الحاجة لمزيد من التوعية حول تأثير مشاركة تفاصيل حياة الأطفال عبر الفضاء الرقمي.

التوصيات:

١- تكثيف الجهود التوعوية حول مخاطر الجرائم المعلوماتية المتعلقة بالحياة الخاصة، من خلال حملات إعلامية وورش عمل توضح أساليب الوقاية منها .
٢- تعزيز القوانين والتشريعات لضمان حماية أقوى للخصوصية، وفرض عقوبات رادعة على مرتكبي الجرائم المعلوماتية
٣- تطوير آليات الإبلاغ عن الجرائم المعلوماتية من خلال منصات سهلة الاستخدام تتيح للأفراد التبليغ بسرية وسرعة .
٤- تعزيز وسائل الأمان الإلكتروني لضمان بيئة رقمية أكثر أمانًا، من خلال تقنيات حديثة تحمي المستخدمين من الاختراقات والانتهاكات.

المقترحات:

١. إجراء دراسات مستقبلية معمقة حول الجرائم المعلوماتية المتعلقة بالحياة الخاصة، مع التركيز على الفئات الأكثر عرضة للخطر، مثل الأطفال والمراهقين .
٢. تحليل أثر القوانين والتشريعات الحالية المتعلقة بالجرائم المعلوماتية، ومدى فعاليتها في الحد من الجرائم المرتبطة بالحياة الخاصة .
٣. دراسة العوامل النفسية والاجتماعية التي تدفع الأفراد لارتكاب الجرائم المعلوماتية، واقتراح استراتيجيات للحد منها.
٤. إجراء دراسات مستقبلية معمقة حول الجرائم المعلوماتية المتعلقة بالحياة الخاصة، مع التركيز على الفئات الأكثر عرضة للخطر، مثل الأطفال والمراهقين .
٥. تحليل أثر القوانين والتشريعات الحالية المتعلقة بالجرائم المعلوماتية، ومدى فعاليتها في الحد من الجرائم المرتبطة بالحياة الخاصة .
٦. دراسة العوامل النفسية والاجتماعية التي تدفع الأفراد لارتكاب الجرائم المعلوماتية، واقتراح استراتيجيات للحد منها.
٧. مقارنة وعي المجتمعات المختلفة حول الجرائم المعلوماتية، لمعرفة الفجوات الثقافية والقانونية التي قد تؤثر على انتشار هذه الجرائم .
٨. البحث في تأثير حملات التوعية والتثقيف على سلوك الأفراد تجاه الجرائم المعلوماتية، ومدى فعاليتها في تعزيز الأمان الرقمي.

المراجع

المراجع العربية

١. الشوابكة، محمد أمين .(2009) .*جرائم الحاسوب والإنترنت* .عمان: دار الثقافة.

٢. الأهواني، حسام الدين كامل .(1978) .*الحق في احترام الحياة الخاصة* .القاهرة: دار النهضة العربية.

٣. البهجي، عصام أحمد .(2005) .*حماية الحق في الحياة الخاصة في ضوء حقوق الإنسان والمسؤولية المدنية (دراسة مقارنة)* .الإسكندرية: دار الجامعة الجديدة للنشر.

٤. الجميلي، فتحية عبد الغني .(2001) .*الجريمة والمجتمع ومرتكب الجريمة* .عمّان: المكتبة الوطنية.

٥. الحسيني، عمر الفاروق .(1995) .*المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية* .القاهرة: دار النهضة العربية.

٦. الخنين، حمد بن عبد الله .(2008) .*الجرائم المعلوماتية وقضاياها المستجدة* .وزارة العدل، ٢٧٦ - ٢٩٦.

٧. الغافري، حسين بن سعيد .(2009) .*السياسة الجنائية في مواجهة جرائم الإنترنت: دراسة مقارنة* . القاهرة: دار النهضة العربية.

٨. المقصودي، محمد بن أحمد بن علي .(2015) .*الجرائم المعلوماتية: خصائصها وكيفية مواجهتها قانونياً – التكامل الدولي المطلوب لمكافحتها* .المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية – ICACC(ص. ٢١–٣٣). الرياض: كلية علوم الحاسب والمعلومات – جامعة الإمام محمد بن سعود الإسلامية.

٩. بنهام، رمسيس .(1999) .*قانون العقوبات "جرائم القسم الخاص."* الإسكندرية: منشأة المعارف.

١٠. تامر، محمد صالح .(2021) .*الابتزاز الإلكتروني (دراسة تحليلية مقارنة)* .المنصورة: دار الفكر والقانون.

١١. الجميلي، فتحية عبد الغني .(2001) .*الجريمة والمجتمع ومرتكب الجريمة* .عمّان: المكتبة الوطنية.

١٢. جميلة، سمير عالية .(2020) .*الجرائم الإلكترونية* .بيروت: منشورات الحلبي الحقوقية.

١٣. سعدات، محمود فتوح محمد .(2015) .*خصائص الجرائم المعلوماتية وصفات مرتكبيها في ظل مجتمع المعلوماتية* .المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية ICACC – (ص. ٣٤–٤٩). الرياض: جامعة الإمام محمد بن سعود الإسلامية - كلية علوم الحاسب والمعلومات.

١٤. صالح، تامر محمد .(2021) .*الابتزاز الإلكتروني (دراسة تحليلية مقارنة)* .المنصورة: دار الفكر والقانون.

١٥. شتا، السيد علي .(1987) .*علم الاجتماع الجنائي* .الإسكندرية: دار المعرفة الجامعية.

١٦. عبدالرحمن، محمود .(1996) .*نطاق الحق في الحياة الخاصة* .القاهرة: دار النهضة العربية.

١٧. عفيفي، عفيفي كامل .(2003) .*جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون (دراسة مقارنة)* .بيروت: منشورات الحلبي الحقوقية.

١٨. فتوش، نقولا .(2004) .*الحق في الحياة الخاصة* .عمان: دار الشروق للنشر والتوزيع.

١٩. فتح الله، محمود رجب .(2019) .*الوسيط في الجرائم المعلوماتية* .الإسكندرية: دار الجامعة الجديدة.

٢٠. لقمان، يمن. (١ نوفمبر، ٢٠٢٣). ارتفاع متهمي الجرائم المعلوماتية. تم الاسترداد من جريدة الوطن السعودية https://www.alwatan.com.sa/article/1136422 :

٢١. لطفي، خالد حسن أحمد .(2018) .*جرائم الإنترنت بين القرصنة الإلكترونية وجرائم الابتزاز الإلكتروني* .الإسكندرية: دار الفكر الجامعي.

٢٢. لجنة الأمم المتحدة الاقتصادية والاجتماعية لغرب آسيا .(n.d.). [ESCWA] *التحرش الإلكتروني* .تم الاسترجاع في ١٠ مارس، ٢٠٢٥، من https://www.unescwa.org/ar/sd-glossary/التحرش-الالكتروني

المراجع الأجنبية

١. Bansal, P. (2018). Cybercrime awareness among prospective teachers in relation to institutional. *Online International Interdisciplinary Research Journal*, 192–198.

٢. Curtin, R. (2021). The effects of response rates on survey quality: Examining gender differences in participation. *Journal of Survey Methodology*, 145–162.

٣. Etikan, I., Musa, S. A., & Alkassim, R. S. (2015). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics*, 5(1), 1–4.

٤. Gupta, G. K. (2014). *Introduction to data mining with case studies* (2nd ed.). New Delhi: PHI Learning Private Limited.

٥. Hinduja, S., & Patchin, J. W. (2015). *Bullying beyond the schoolyard: Preventing and responding to cyberbullying* (2nd ed.). Sage Publications.

٦. Kowalski, R. M., Limber, S. P., & Agatston, P. W. (2014). *Cyberbullying: Bullying in the digital age* (2nd ed.). Chichester, West Sussex: Wiley-Blackwell.

٧. Lindemann, D. J. (2019). Gender differences in survey response behavior: Analyzing trends in participation. *Social Research Quarterly*, 233–250.

٨. Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2013). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health and Mental Health Services Research*, 40(6), 533–544.

٩. Smith, T. W. (2020). Understanding gender-based variations in survey engagement. *Journal of Applied Social Research*, 87–105.

١٠. Symantec. (2019). *Internet Security Threat Report* (Vol. 24). Symantec Corporation. https://www.symantec.com/security-center

١١. UNICEF. (2024). *Cyberbullying: What is it and how to stop it*. Retrieved from https://www.unicef.org/end-violence/how-to-stop-cyberbullying

١٢. Van der Hulst, R. C., & Neve, R. J. M. (2008). *High volume cyber crime and the organization of the police: The results of two empirical studies in the Netherlands*. Amsterdam, Netherlands: Kloof Booksellers & Scientia Verlag.

١٣. Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4*(5), 193–220.