اتجاهات الشباب الكويتي نحو أهمية الأمن السيبراني في ضوء مخاطر انتهاكات الخصوصية عبر تطبيقات ومنصات الإعلام الجديد

د. سالم صباح الشمري*

ملخص الدراسة:

استهدفت الدراسة بشكل رئيس التعرف على اتجاهات الشباب الكويتي نحو أهمية الأمن السيبراني.. في ضوء مخاطر انتهاك الخصوصية عبر تطبيقات ومنصات الإعلام الجديد، تنتمي هذه الدراسة إلى البحوث الوصفية، كما اعتمدت على منهج المسح، وتم تطبيقها على عينة مكونة من 400 مفردة من الشباب الكويتي.

وتوصلت الدراسة إلى عدة نتائج، أبرزها:

- ارتفاع مستوى حرص المبحوثين عينة الدراسة على تأمين وحماية بياناتهم الشخصية عبر تطبيقات ومنصات الإعلام الجديد التي يستخدمونها
- أن المبحوثين عينة الدراسة لا يثقون بالشكل الكافي في أمان بياناتهم ومعلوماتهم عبر تطبيقات ومنصات الإعلام الجديد التي يستخدمونها
- أن اتجاه المبحوثين عينة الدراسة جاء مرتفعاً نحو مفهوم الأمن السيبراني وانتهاك الخصوصية لديهم.
- أظهر المبحوثون عينة الدراسة ايجابيتهم حال تعرضهم لاختراق خصوصيتهم عبر أحد تطبيقات ومنصات الإعلام الجديد التي يستخدمونها.
- أرجع المبحوثين عينة الدراسة انتشار جرائم انتهاك الخصوصية عبر تطبيقات ومنصات الإعلام الجديد إلى عدة أسباب، وفي مقدمتها"عدم اكتشاف هذه الوقائع إلا بعد فترة زمنية طويلة بما يصعب تجنبها".

الكلمات المفتاحية: (الأمن السيبراني، انتهاك الخصوصية، الشباب الكويتي، الإعلام الجديد)

* دكتور في علوم الاتصال الحديثة والاعلام (مقدم برامج)- وزارة الإعلام الكويتية

Attitude of Kuwaiti youth towards the importance of cyber security In light of the risks of privacy violations across new media apps and platforms

Dr. Salem Sabah Al-Shammari*

Abstract:

The study sought to determine the attitudes of Kuwaiti youth towards the importance of cybersecurity.. in light of the risks of privacy violations through new media applications and platforms. This study belongs to descriptive research, and it relied on the survey method, and was applied to a sample of 400 Kuwaiti respondents. The study concluded to some important results as follows:

- The high level of interest of the study sample respondents in securing and protecting their personal data through social media apps.
- The respondents do not trust the security of their data and information through the new media applications and platforms they use.
- Increase the study sample respondents' awareness of the concepts related to cybersecurity and privacy violations.

Keywords: (Cybersecurity, Privacy Violation, Kuwaiti Youth, New Media)

* Doctor of Modern Communication and Media Sciences (program presenter), Kuwaiti Ministry of Information

مقدمة:

على الرغم من الإيجابيات الهائلة التي تحققت بفضل تقنية المعلومات، فإن تلك الثورة المعلوماتية المتصاعدة قد صاحبتها في المقابل جملة من الانعكاسات السلبية الخطيرة نتيجة سوء الاستخدام، ومن بين تلك الانعكاسات المستحدثة، ظاهرة الجريمة الرقمية، وعلى رأسها انتهاك الخصوصية، والتي تصاعدت أخطارها بدورها مما أفرز نوعا جديدا من الجرائم العابرة للقارات، التي لم تعد أخطارها وأثارها محصورة في نطاق دولة بعينها، الأمر الذي أثار بعض التحديات أمام الأجهزة المعنية بمكافحة الجريمة.

إن قضية أمن وحماية المعلومات تعتبر من أهم قضايا عصر الثورة الصناعية الرابعة، حيث أصبح نجاح أي مؤسسة يعتمد بشكل كبير على ما تمتلكه من معلومات، لكن العديد من المعلومات والأنظمة والبني التحتية المتصلة بالشبكات عرضة للخطر بين الحين والآخر، حيث تواجه بأنواع شتى من الخروقات للمعلومات، كما تتعرض لأنشطة إجرامية (هاكرز) تعطل خدماتها وتدمر ممتلكاته، وتختلف هذه الاختراقات من جهة لأخرى ومن مكان لآخر ومن زمن إلي زمن مستخدمة أدوات وآليات متجددة ومتطورة طول الوقت[1].

إن استخدام التقنيات الحديثة بين المؤسسات والأفراد على حد سواء، وقدرتها الهائلة على تخزين ومعالجة البيانات والمعلومات وسهولة استرجاعها، والتوجه نحو الاعتماد على المعلومات والبيانات كأحد متطلبات الاقتصاد المعرفي ساهم ذلك في التوسع في انتهاكات خصوصية الأفراد، وتعدد أشكاله، وبعد أن كان الحديث يدور عن الحق في الاتصال، والحق في المعرفة والحصول على المعلومة، أصبح يدور حول حماية حقوق الإنسان من مخاطر الإعلام الجديد، لا سيما الحق في الخصوصية وحرمة الحياة الخاصة، فبيانات المستخدمين ومعلوماتهم الشخصية واتصالاتهم، تخزن وتجمع إلكترونيا، ليس من إدارة الشبكة والشركات المختصة فحسب من كل من له القدرة والإمكانية على ذلك سواء كان من الهاكرز أو مزودي الخدمة أو الحكومة أو دول وشركات أخرى، فضلا عن ما أتاحته هذه الوسائل من مزايا مكنت مستخدميها من انتهاك خصوصية بعضهم البعض ونشر ما يريدون تحت أسماء مستعارة، ودون وضع اعتبارات[2].

وفي ضوء تزايد الاستخدام والاعتماد على البيئة الرقمية ومنصاتها وتطبيقاتها المختلفة، تظهر الحاجة إلى وجود آليات لحماية البيانات والمعلومات الشخصية للمستخدمين، فالحصول عليها وانتهاكها قد يسبب أضرارا بالغة نفسياً ومادياً، وتتعاظم تلك الأهمية إذا ارتبط ذلك بفئة الشباب، فهم الأكثر استخداما لشبكة الإنترنت، والأكثر استهدافا من جانب منتهكي الخصوصية، ومعرفة مدى وعيهم بالأمن السيبراني، وأهميته في حماية بياناتهم، وطرق الحماية، وهو مجال الدراسة الحالية، التي قد تقدم نتائجها فائدة يمكن من خلالها تجنب وقوعهم ضحايا لمجرمي الانترنت.

مشكلة الدراسة:

خلال الأعوام الماضية أدركت الدول أهمية الأمن السيبراني في حماية بيانات أفرادها ومؤسساتها، وأيقنت أن التسليح العسكري لم يعد هو فقط معياراً لقياس قوة الدولة، وقد انعكس ذلك على اهتمامها بهذا المجال، وعملت على رفع وعي الشعوب بأهميته والمخاطر الناجمة عن تجاهله وعدم المعرفة به، من خلال المبادرات المعرفية عبر وسائل ومنصات الإعلام المختلفة، حيث تزداد مخاطره في ظل التطور التكنولوجي المستمر في وسائل الاتصال، واعتماد المجتمعات الحديثة بشكل متزايد على تقنيات الاتصالات والمعلومات عبر شبكة الانترنت، وهذا الاعتماد يتواكب مع وجود مخاطر محتملة تهدد بشكل رئيس أمن المعلومات للمجتمع والأفراد على حد سواء، ترتبط هذه المخاطر كثيراً بتزييف المحتوى وانتهاك خصوصية الأفراد وسرقة بياناتهم ومعلوماتهم، وانتحال صفتهم، وبصفة خاصة فئة الشباب حيث تعد الأكثر استخداماً والأكثر استهدافاً، لذا كان من الضرورة التعرف على اتجاهات الشباب الكويتي نحو أهمية الأمن السيبراني، وكيفية حمايتهم لبياناتهم الشخصية من الاختراق، وفي ضوء ذلك يمكن بلورة مشكلة الدراسة في التساؤل التالي: **ما اتجاهات الشباب الكويتي نحو أهمية الأمن السيبراني.. في ضوء مخاطر انتهاك الخصوصية عبر تطبيقات ومنصات الإعلام الجديد.**

أهمية الدراسة:

تكمن أهمية الدراسة الحالية في كونها من الدراسات العلمية التي تهدف إلى التعرف على اتجاهات الشباب الكويتي نحو الأمن السيبراني، ومخاطر تزييف المحتوى وانتهاك الخصوصية عبر تطبيقات ومنصات شبكة الانترنت، إلا أن تلك الأهمية تبرز في المجالين النظري والتطبيقي وذلك على الوجه التالي:

أولاً: الأهمية النظرية.

- قلة الدراسات التي تناولت مفهوم الأمن السيبراني في المجال الإعلامي بدولة الكويت، بالرغم من أهميته، ومخاطره التي تتجاوز أمن الأفراد لتمس الأمن القومي للبلاد.
- في ظل تزايد التهديدات والتحديات المستقبلية في المجال السيبرانى والمجتمع الرقمي تقدم الدراسة إطاراً نظريا يساعد على فهم ومجابهة المخاطر والتهديدات المتزايدة في المستقبل.
- قد تقدم نتائج الدراسة معلومات للمختصين تساعدهم في إعداد البرامج التوعوية للجمهور حول مخاطر الأمن السيبراني، وكيفية الاستخدام الآمن للتطبيقات والمنصات عبر شبكة الإنترنت.
- تسلط الدراسة الضوء على التحديات التي تواجه الشباب في معرفتهم بالأمن السيبراني، وأهمية توعيتهم بمخاطره.

- أهمية الفئة العمرية التي تستهدفها الدراسة وهي فئة (الشباب)، حيث أنهم يمثلون القوة في المجتمع، والشريحة الأكبر في تشكيله، والأكثر تأثيراً وتأثرا عبر شبكة الإنترنت وتطبيقاتها ومنصاتها المختلفة.

ثانياً: الأهمية التطبيقية.

- إن جرائم المتعلقة بالأمن السيبراني أصبحت أولوية قصوى للدول في إدارة أمنها القومي، فقد يتم استهداف الدول وإسقاطها إلكترونيا عبر فضائها الإلكتروني، وليس عسكرياً عبر حدودها البرية أو البحرية أو الجوية، وهو ما يعظم من أهمية دراسة القضايا المتعلق بالأمن السيبراني.
- تزايد الهجمات السيبرانية ومخاطرها على أمن المعلومات والبيانات للدول والأفراد المستخدمين لشبكة الانترنت، كما تتزايد تكلفتها مادياً ومعنوياً، ودراستها وتقديم معرفة حولها قد يساعد في رفع الوعي بخطورتها.
- يمثل الشباب الفئة الأكثر استخداما لشبكة الإنترنت من خلال التطبيقات والمنصات المختلفة، وبالتالي هم الأكثر استهدافا من جانب قراصنة الإنترنت، والتعرف على اتجاهاتهم نحو الأمن السيبراني يمثل ضرورة للوقوف على مدى معرفتهم به، وكيفية محافظتهم على أمنهم المعلوماتي.
- توفر الدراسة الإطار العملي لفهم طبيعة الشباب وكيفية تعاملهم مع محاولات اختراق خصوصياتهم عبر شبكة الإنترنت وتعزز من تحسين ممارساتهم وسلوكياتهم في استخدامهم لها.

أهداف الدراسة:

تستهدف الدراسة بشكل رئيس التعرف على اتجاهات الشباب الكويتي نحو أهمية الأمن السيبراني.. في ضوء مخاطر انتهاك الخصوصية عبر تطبيقات ومنصات الإعلام الجديد، ويندرج تحت هذا الهدف، عدة أهداف فرعية كالآتي:

- التعرف على مدى معرفة الشباب الكويتي بموضوع الأمن السيبراني.
- الكشف عن تصورات الشباب الكويتي عن مفهوم الأمن السيبراني، والجرائم المرتبطة به.
- تحديد مدى معرفة الشباب الكويتي بمخاطر انتهاك الخصوصية عبر استخدامهم لتطبيقات ومنصات الانترنت المتعددة، وآليات التعامل الآمن في استخدامهم لها.
- التعرف على مقترحات الشباب الكويتي نحو كيفية تعزيز الأمن السيبراني والحد من مخاطره.
- تحديد المصادر التي يعتمد عليها الشباب الكويتي في الحصول على معلوماتهم حول الأمن السيبراني.
- الكشف عن الفروق في مستوى معرفة الشباب الكويتي بالأمن السيبراني ومخاطر انتهاك الخصوصية وفقا للمتغيرات الديموغرافية لهم (النوع، السن، المستوى التعليمي).

الدراسات السابقة:

سوف يعرض الباحث الدراسات السابقة من خلال محورين، يتناول المحور الأول منهما: الدراسات التي بحثت في موضوع الأمن السيبراني، ويتناول المحور الثاني: الدراسات التي استهدفت دراسة انتهاك الخصوصية عبر تطبيقات ومنصات الإعلام الجديد.

المحور الأول: دراسات تناولت الأمن السيبراني.

ناقشت العديد من الدراسات الإعلامية موضوع الأمن السيبراني، وتنوعت أهداف هذه الدراسات، وأدواتها المنهجية، كما تباينت نتائجها، ومن ذلك **دراسة (Mrittika Rani، 2024)**، التي توصلت إلى وجود علاقة ارتباطية ذات دلالة إحصائية ايجابية بين معرفة الطلاب بالأمن السيبراني وأمان كلمة المرور، ويزداد ذلك كلما ارتفع مستوى وعيهم بالأمن السيبراني، أكد تحليل البيانات أن موقف الأمن السيبراني يتوسط العلاقة بين معرفة الأمن السيبراني وأمان كلمة المرور.

ولتحقيق أهداف الدراسة المتعلقة بالكشف عن كيفية تأثير معرفة طلاب الجامعات في بنغلاديش بالأمن السيبراني وأمان كلمة المرور والتصور الذاتي لديهم على قضايا الوعي بالأمن السيبراني، تم إجراء دراسة من خلال استبيان على عينة عشوائية طبقية مكونة من 430 طالبًا جامعيًا من جامعتين حكوميتين وثلاث جامعات خاصة البيانات في دكا، ببنغلاديش، واستخدمت الدراسة المنهج الوضعي، وتم استخدام تقنية الاستدلال الإحصائي الافتراضية، ومن خلال التحليل الكمي للبيانات وتوصلت النتائج إلى ضرورة بذل المزيد من الجهود لتوعية عامة الناس من الطلاب وغيرهم حول الأمن السيبراني والاستخدام الأخلاقي للإنترنت، بالإضافة إلى ضرورة المساهمة الفاعلة والرئيسة في التأكيد على الحاجة إلى زيادة الوعي بالأمن السيبراني بين جمهور الطلاب لأنهم الأكثر استخداما للتكنولوجيا الحديثة، والأكثر وقوعا في الأخطاء والأضرار التي تسببها الانتهاكات غير الأخلاقية للأمن المعلوماتي[3].

وفي ذات السياق جاءت **دراسة (مطلق سعد العميري، 2024)**، التي استهدفت الوصول إلى الاستراتيجيات التي يوظفها الإعلام الإلكتروني بالكويت تجاه الأمن السيبراني، وبحث العوامل المؤثرة في مخططات الإعلام الإلكتروني تجاه الأمن السيبراني في الكويت، واستندت الدراسة إلى المنهج الوصفي واستمارة الاستبيان بوصفها أداة لتحصيل البيانات، وقد تكونت عينة البحث من 150 مفردة من العاملين في الصحف الكويتية الإلكترونية ووكالة الأنباء الكويتية (كونا) والمواقع الإعلامية الحكومية الكويتية والقائمين عليها، وقد انتهت الدراسة إلى أن ارتفاع مستوى المخططات التي يوظفها الإعلام الإلكتروني الكويتي تجاه الأمن السيبراني، حيث يتم الإبلاغ عن المواقع التي تجسد الأخبار الزائفة وكشف بؤر ومخطط المنظمات الإرهابية، وتعريف الجمهور بالعقوبات والقوانين الرادعة لمرتكبي التهديدات السيبرانية، كما أن واقع استعمال العاملين في الصحافة الكويتية الإلكترونية والمواقع الإعلامية الحكومية الكويتية من مخططات تجاه الأمن السيبراني جاء مرتفعا، وهذا يدل على ارتفاع درجة استعمال الكوادر المبحوثة للاستراتيجيات تجاه الأمن السيبراني حيث تسعى الصحف والمواقع الكويتية الإلكترونية إلى وجود الدعم الفني كأحد أساسيات الأمن السيبراني للأنظمة الإدارية وقد توفر

الصحف والمواقع الكويتية الإلكترونية إدارة خاصة بالأمن السيبراني، واقترحت الدراسة زيادة وعي العاملين الإعلام الإلكتروني بمخاطر الاعتماد على الأجهزة الشخصية كالهواتف المحمولة لتخزين البيانات السرية المتعلقة بالعمل، وامتلاك لنظام حوكمة تقني لتوفير الأمن السيبراني للتعاملات الإلكترونية، وتشديد العقوبات على جرائم الفضاء السيبراني، وتوفير المزيد من الدعم الفني بوصفه أحد الأساسيات لتحقيق الأمن السيبراني للبيانات الإدارية[4].

ولتقييم مدى فعالية استخدام وسائل التواصل الاجتماعي لرفع مستوى الوعي بالسلامة السيبرانية بين أفراد الجمهور، وإمكانية استخدامها في رفع وعي الجمهور بمخاطر انتهاكات الخصوصية وأهمية الأمن السيبراني بوصفها أكثر وسائل الاتصال استخداما بين الجمهور، كشفت **دراسة (Anakha Prakash، 2024)**، أنه يمكن تسخير المنصات باعتبارها التيار الرئيسي لحملات التوعية بالأمن السيبراني لتعزيز معرفة الجمهور بالمواقف والممارسات المتعلقة بعادات السلامة عبر الإنترنت، وأنه على الرغم من أن الكثير من الناس يعتمدون على التكنولوجيا الرقمية بشكل متزايد، إلا أنه لا يزال هناك الكثير منها الأشخاص الذين ليس لديهم معرفة بكيفية الحفاظ على أمانهم أثناء الاتصال بالإنترنت، فهناك تفاوتاً بين المبحوثين في درجة معرفتهم ووعيهم بالأمن السيبراني.

وأكدت نتائج الدراسة التي استخدمت أساليب البحث الكمي والكيفي لتحليل منشورات وسائل التواصل الاجتماعي المتعلقة بالسلامة السيبرانية، لتحليل لقاءات مع أشخاص تعرضوا لحملات توعوية خاصة بتعريفهم بالأمن السيبراني ومخاطر سرقة البيانات، وتم إجراء الدراسة على عينة من الجمهور بالهند ممن تتراوح أعمارهم بين 18: 65 عام، أن حملات التوعية من خلال وسائل التواصل الاجتماعي نجحت بشكل كبير في رفع وعي الجمهور بالأمن السيبراني ومخاطر انتهاك الخصوصية وسرقة البيانات، كما ينبغي مراعاة العوامل الديموغرافية مثل العمر أو الجنس أو مستوى التعليم وما يتعلق بمحو الأمية الرقمية عند تصميم حملة فعالة للسلامة السيبرانية من خلال وسائل التواصل الاجتماعي[5].

وحول الكشف عن احتمالية مدى وقوع مستخدمي الانترنت كضحايا لهجمات القرصنة الالكترونية، ومدى معرفتهم ووعيهم بالأمن السيبراني وأهميته في الحفاظ على بياناتهم ومعلوماتهم، جاءت **دراسة (Mengqi Liao، 2023)**، والتي توصلت من خلال المقارنة بين مجموعتين من المستخدمين، المجموعة الأولى وهم مستخدمي الانترنت عبر الهواتف الذكية، والمجموعة الثانية مستخدمي الانترنت عبر أجهزة الكمبيوتر، إلى أن مستخدمي الانترنت عبر الهواتف المحمولة هم أكثر سرعة في معالجة البيانات والمعلومات، وأقل عرضة من الوقوع في الهجمات السيبرانية، على عكس أولئك الذين يستخدمون شبكة الانترنت عبر أجهزة الكمبيوتر، حيث يقعون ضحايا لقراصنة الانترنت، لأنهم أكثر دخولاً على الروابط المجهولة التي تصل إليهم عبر البريد الإلكتروني أو منصات التواصل الاجتماعي.

كما أوضحت الدراسة التي تقع ضمن الدراسات الوصفية، واستخدمت منج المسح لإجراء الدراسة على عينة مكونة من (131) مبحوثاً بولاية بنسلفانيا الأمريكية، أن مستخدمي الانترنت عبر الكمبيوتر أكثر وعيا من نظرائهم المستخدمين للشبكة عبر الهواتف المحمولة، لكن القراصنة غالبا من يعرفون ذلك ويطورون من أدواتهم لسرقة بيانات ومعلومات المستخدمين،

واقترحت الدراسة أن يتم استخدام الأجهزة المحمولة في رفع مستوى وعي المستخدمين للانترنت من خلالها بتوجيه حملات توعية مستمرة لهم في كيفية التعامل الصحيح مع هذه الهجمات وكيفية مكافحة الخداع والتضليل الالكتروني(6).

وفي ذات الاتجاه جاءت **دراسة (هدير محمود، 2023)**، والتي توصلت من خلال قياس مستوى معرفة مستخدمي الانترنت بسياسات وإجراءات أمن المعلومات ومدى تأثير هذه المعرفة على اتجاههم وسلوكيات حمايتهم لأمنهم السيبراني، والوقوف على مدى تأثير الاتجاه، درجة ميل الأشخاص للمخاطرة، وسمات الشخصية الخمس الكبرى " الانبساط، القبول والمسابرة، والضمير، والعصابية، والانفتاح" على العلاقة بين مستوى معرفة مستخدمي الانترنت بسياسات وإجراءات أمن المعلومات وسلوكيات حمايتهم لأمنهم السيبراني، والتعرف على مدى تأثير العوام الديموغرافية على مستوى معرفة المستخدمين بهذه السياسات وسلوكهم نحوها، إلى أن درجة معرفة المبحوثين بسياسات وإجراءات أمن المعلومات تتراوح بين متوسطة إلى مرتفعة، وأن نسبة 76% من المبحوثين لديهم تجاه ايجابي نحو حماية أمنهم السيبراني، وأن نسبة 68% كان لديهم مستوى مرتفع من الالتزام بسلوكيات حماية الأمن السيبراني، وأن أكثر من نصف العينة لديهم مستوى مرتفع من الميل للمخاطرة، وأن غالبية المبحوثين يرون أنهم يتسمون بسمات القبول أو المثابرة.

وعبر نموذج المعرفة_الاتجاه_ السلوك، الذي اعتمدت عليه الدراسة، ومنهج المسح لتطبيق الدراسة من خلال استبانة على عينة قوامها 400 مفردة من مستخدمي الإنترنت ممن تبلغ أعمارهم 18 سنة فأكثر، أثبتت الدراسة وجود علاقة طردية بين مستوى المعرفة بسياسات وإجراءات امن المعلومات واتجاههم نحو حماية أمنهم السيبراني، أي أنه كلما زادت معرفة الأفراد بسياسات وإجراءات أمن المعلومات زاد التزامهم بسلوكيات الحماية لأمنهم السيبراني، كما حددت النتائج بعض المتغيرات التي تؤثر على العلاقة بين المعرفة والسلوك السيبراني للأفراد(7).

وللتعرف على العلاقة بين الإعلام الرقمي والأمن السيبراني والدور الفعال الذي يقوم به الإعلام الرقمي في دعم وتعزيز الأمن السيبراني، والكشف عن طبيعة الأمن السيبراني وأهم المفاهيم المرتبطة به وكذلك التعرف على التهديدات والجرائم السيبرانية التي يتم يمكن التعرض لها، والوقوف على طرق مكافحة تلك التهديدات والجرائم التي تؤثر بالسلب على الاستقرار والتقدم نحو التنمية المستدامة، جاءت **دراسة (شيرين عبد الحفيظ، 2023)**، والتي توصلت إلى أن الإعلام الرقمي له دور كبير في تعزيز الأمن السيبراني، وأن الإعلام الرقمي يؤدي دورا كبيرا في مقاومة التهديدات والجرائم السيبرانية، وأن العلاقة بين الأمن السيبراني والمحتوى المعلوماتي علاقة قوية فكلما زاد المحتوى المعلوماتي والعسكري والأمني والفكري والسياسي والاجتماعي والاقتصادي والخدمي والعلمي زادت أهمية الأمن السيبراني الذي أصبح من الضروريات الأساسية التي لا غنى عنها وأن الإعلام الجديد يلعب دور رأس الحربة في تدعيم وتعزيز الأمن السيبراني ومقاومة التهديدات والجرائم والتهديدات والجرائم السيبرانية، كما يساهم الإعلام الرقمي بإيجابية في العمل على تشجيع الدول نحو التحول الرقمي وتطبيق الرقمنة لدى جميع المؤسسات والهيئات والحكومات الشركات وإلزامهم بذلك.

وأوضحت نتائج الدراسة التي اعتمدت على نظرية انتشار المستحدثات، وتنتمي إلى الدراسات الاستكشافية والوصفية، واستخدمت منهج المسح وأداة الاستبيان لجمع البيانات من (64) مفردة من الإعلاميين المتخصصين في تخصصات مختلفة (الصحافة ،الإذاعة والتليفزيون) بالمؤسسات الإعلامية (مؤسسة الأهرام وأخبار اليوم ، الجمهورية والإذاعة والتليفزيون)، ضرورة وضع استراتيجيه متكاملة لمكافحة التهديدات والجرائم السيبرانية وقيام المستخدمين بالفهم العميق للطرق والأساسيات اللازمة لأمان البيانات والمعلومات وتنفيذ خطوات الأمان وفي مقدمتها اختيار كلمات مرور قوية، كما أوصت الدراسة بضرورة القيام بتأهيل كوادر مدربة تكون متخصصة في الأمن السيبراني ومتعمقة في مجال الفضاء السيبراني، لتمثل حائط صد قوى للتهديدات والجرائم السيبرانية(8).

وفيما يرتبط بالتعرف على قضايا الأمن السيبراني التي حظيت باهتمام وسائل الإعلام الجديد عينة الدراسة، ورصد أبرز الهجمات السيبرانية ومخاطرها، ومعرفة تداعيات الهجمات السيبرانية على الأمن القومي، والتعرف على السبل والإمكانيات المتاحة لمواجهة تلك الحروب، ورصد الآليات الإعلامية في مكافحة تلك الجرائم، جاءت **دراسة (أماني حمدي، إيمان عبد المنعم، 2022)**، التي أكدت أن قضيتي اختراق الحسابات والاستخدامات الإيجابية جاءت في الترتيب الأول من حيث القضايا الفرعية التي اهتمت بها وسائل الإعلام الرقمي عينة الدراسة في مكافحة الجرائم السيبرانية، وأضافت الدراسة التي تعد من الدراسات الوصفية التحليلية، واستخدمت المنهج الوصفي التحليلي، والمنهج المقارن، وأداتي: التحليل الاستراتيجي، وتحليل المضمون، وتم إجراءها خلال فترة زمنية استمرت 6 أشهر، أن أهم مصادر المعلومات في مواقع الإعلام الرقمي عينة الدراسة في مكافحة الجرائم السيبرانية هي المواقع الإلكترونية الإخبارية، والصفحات الرسمية التابعة لمؤسسات وهيئات حكومية، وجاء في مقدمة أساليب المعالجة في مواقع الإعلام الرقمي عينة الدراسة في مكافحة الجرائم السيبرانية هي إبراز إطار الايجابيات ثم إطار السلبيات، وأن من أهم آليات المعالجة التي اعتمدت عليها عينة الدراسة تمثلت في الخدمات التي تطرحها الصفحات جاءت "خدمي" ، ثم توعوي، ثم تثقيفي(9).

كما استهدفت **دراسة (بشائر حامد ، أمال سعد الدين، 2021)** قياس معرفة الصحفيين بموضوع الأمن السيبراني، والتعرف على الأبعاد التي يتناولها الأمن السيبراني في الوقت الراهن من وجهة نظرهم، وتحديد مدى معرفة الصحفيين بتطبيقات الأمن السيبراني في المملكة العربية السعودية، وقياس معرفتهم بالأنظمة والتشريعات التي تتعلق بالفضاء السيبراني، وتقييم تغطية الصحف السعودية في توعيتها بمفهوم الأمن السيبراني ومعرفة جانب القوة والضعف، وتحديد الأشكال الصحفية التي اعتمدت عليها هذه الصحف في معالجة قضية الأمن السيبراني، والكشف عن مد معرفة الصحفيين باختصاصات ومهام الهيئة الوطنية للأمن السيبراني في المملكة، تنتمي هذه الدراسة إلى حقل الدراسات الوصفية، واعتمدت على استمارة الاستبيان لجمع البيانات من المبحوثين البالغ عددهم (42) مفردة من الصحفيين السعوديين.

وتوصلت الدراسة إلى أن الصحفيين السعوديين على دراية بالأمن السيبراني حيث بلغت نسبتهم 84% من جملة المبحوثين، وأن هناك فروقا بين المبحوثين في مدى معرفتهم بمهام ووظائف

الهيئة الوطنية للأمن السيبراني، حيث بلغت نسبة من أجابوا " بمعرفتهم بدرجة متوسطة " 42%، كما أكدت الدراسة وجود فروق بين المبحوثين في مدى معرفتهم بالأنظمة والتشريعات المتعلقة بالأمن السيبراني حيث بلغت نسبة من يعرفونها " بدرجة متوسطة" 49%، ويرى المبحوثين أنه يجب تحديد قائمة بالتشريعات والتنظيمات المتعلقة بالأمن القومي والمتطلبات ذات الصلة وتوثيقها وتحديثها دوريا، وأن الهيئة الوطنية للأمن السيبراني جاءت في مقدمة المصادر التي يعتمدون عليها في تغطية الموضوعات المتعلقة بالأمن السيبراني، وان الخبر الصحفي جاء في مقدمة الأشكال الصحفية التي يقدمون من خلالها الموضوعات المتعلقة بالأمن السيبراني[10].

واستهدفت **دراسة (Nnamdi O. Madichie، 2021)**، معرفة مدى امتثال الموظفين للأمن السيبراني وسياساته، وقد طبقت الدراسة على عينة من مجتمع الموظفين متعددة الثقافات والجنسيات في الولايات المتحدة وبريطانيا والإمارات العربية المتحدة، بلغ قوامها 3732 مفردة من خلال الاستبيان الإلكتروني، وقد استخدمت الدراسة نموذج يسمى نموذج الامتثال لأمان الهاتف الذكي والذي يهدف إلى معرفة عمق وفهم سلوك أمن المعلومات للموظفين، واستكشاف التأثيرات الوطنية والتنظيمية والتكنولوجية الخاصة بالهواتف الذكية والشخصية.

وقد توصلت نتائجها إلى ضرورة الاستخدامات الآمنة للهواتف الذكية لدى الموظفين في العمل مع مراعاة الاختلافات الثقافية والمعرفية بين الجنسيات المختلفة وكذلك التحذير من التهديدات والجرائم السيبرانية عبر الهواتف الذكية، كما أن اتخاذ شركات الهواتف الذكية لمزيد من الاحتياطات في تطبيقات الأمن يساعد على بناء ثقة قوية بينها وبين عملائها، ويقدم صور ايجابية عنها ترفع من مستوى ثقتهم فيها، وتعزز سمعتها الحسنة لديهم[11].

كما كشفت **دراسة (آية عبد الهادي، 2021)** عن العلاقة بين استخدام مواقع التواصل الاجتماعي والوعي بأهمية الأمن السيبراني، وإدراكهم لأهمية الأمن السيبراني ودوره في الأمن المعلوماتي، وطرق المحافظة على البيانات والمعلومات، وتحديد معدلات استخدامهم لمواقع التواصل الاجتماعي ودوافعهم في ذلك، وتوصلت نتائج الدراسة إلى أن أغلبية مستخدمي مواقع التواصل الاجتماعي (عينة الدراسة) يتراوحون بين أنهم يدركون الأمن السيبراني وطرق المحافظة على نظامه بدرجة متوسطة ومرتفعة، وأن أغلبية مستخدمي مواقع التواصل الاجتماعي (عينة الدراسة) يتراوحون بين أنهم يدركون مخاطر الأمن السيبراني وانتهاكاته بدرجة مرتفعة ومتوسطة، وأن هناك علاقة ارتباطية دالة إحصائيا بين معدلات استخدام مواقع التواصل الاجتماعي والمتغيرات التالية: (دوافع استخدام مواقع التواصل الاجتماعي/ إدراك مستخدمي مواقع التواصل الاجتماعي للأمن السيبراني/ إدراك مستخدمي مواقع التواصل الاجتماعي لطرق المحافظة على نظام الأمن السيبراني/ إدراك مستخدمي مواقع التواصل الاجتماعي لمخاطر الأمن السيبراني/ إدراك مستخدمي مواقع التواصل الاجتماعي لانتهاكات الأمن السيبراني).

وأضافت الدراسة التي تعد من الدراسات الوصفية، واستخدمت منهج المسح الكمي، واعتمدت على استمارة الاستبيان لجمع البيانات من عينة عمديه قوامها (440 مفردة) من مستخدمي مواقع التواصل الاجتماعي من مختلف الأعمار والمستويات التعليمية، والاقتصادية،

والاجتماعية، أن هناك علاقة ارتباطية دالة إحصائيا بين إدراك مستخدمي مواقع التواصل الاجتماعي للأمن السيبراني و إدراكهم لطرق المحافظة على نظامه ومخاطره وانتهاكاته، وأن هناك علاقة ارتباطية دالة إحصائيا بين إدراك مستخدمي مواقع التواصل الاجتماعي لطرق المحافظة على نظام الأمن السيبراني وإدراكهم لمخاطره وانتهاكاته، وأن هناك علاقة ارتباطية دالة إحصائيا بين إدراك مستخدمي مواقع التواصل الاجتماعي لمخاطر الأمن السيبراني وإدراكهم لانتهاكات الأمن السيبراني[12].

وفي السياق ذاته استهدفت **دراسة (نهي مجدي، 2021)**، التعرف على العلاقة بين المضمون الإعلامي ودوره في تحقيق الأمن السيبراني في ظل رؤية مصر 2030، وشرح مفهوم الأمن السيبراني والتهديدات الإلكترونية ومخاطر استخدام الإنترنت، وتحديد طبيعة جرائم الاتصال عبر الإنترنت ذات الصلة بوسائل الإعلام، ومعوقات وصعوبات ضبط المضمون الإعلامي لدعم تحقيق الأمن السيبراني، واستخدمت الدراسة المنهج الوصفي التحليلي بتطبيق استبانة على عينة عمدية من 32 من أساتذة وخبراء الإعلام والتقنية بكليتي الإعلام والهندسة.

وقد توصلت نتائجها إلى وجود اتجاه إيجابي للإعلاميين وخبراء التقنية والاتصال نحو العلاقة بين الأمن السيبراني ومضمون الرسالة الإعلامية، وتمثلت معوقات وصعوبات ضبط المضمون الإعلامي لدعم تحقيق الأمن السيبراني في غياب الجهة الموحدة المنظمة، وضعف آليات الرقابة والتشريعات المرتبطة بها، والحاجة إلى قانون دولي يحكم الانحرافات، كما تم تحديد دور الإعلام في تحقيق الأمن السيبراني انطلاقاً من رؤية مصر 2030 في زيادة الوعي والتثقيف والتحذير لخلق القاعدة الشعبية القادرة على مواجهة التهديدات السيبرانية.

وأشارت النتائج إلى أنه لا يوجد استقرار نسبي فيما يتعلق بمعايير رقابة المضمون الإعلامي كما أنه هناك قلة دراية من بعض الإعلاميين بمخاطر الأمن السيبراني وإجراءات الردع، فضلا عن عدم وجود إجراءات وتشريعات كافية لضبط المضمون الإعلامي بما يدعم تحقيق الأمن السيبراني، وكذلك عدم وجود القدر الكافي من الجهات الرسمية المشتركة بين الإعلاميين وخبراء التقنية تساعد في عملية تحقيق الأمن السيبراني، كما أيدت الأغلبية عدم كفاية القوانين والتشريعات التي يصدرها مجلس الإعلام بالتنسيق مع خبراء تقنية الاتصال لدعم تحقيق الأمن السيبراني بنسبة، وكان هناك اتجاه بأنه على الإعلام الاضطلاع بدور الوعي الثقافي بالمخاطر السيبرانية وكذلك أهمية لوضع التشريعات التي تعزز من تحقيق الأمن السيبراني[13].

وفي هولندا استهدفت **دراسة Kleij، R. van der ، (2021)**، التعرف على مدى معرفة الجمهور الهولندي بالأمن السيبراني، وتفسير سلوكيات المبحوثين عينة الدراسة من خلال قدراتهم المختلفة، وفرصهم المتاحة، ودوافعهم، نحو الأمن السيبراني والاختراقات المحتملة بياناتهم الخاصة، وتم استخدام منهج المسح، واستمارة الاستبيان لتطبيقها على عينة مكونة من (2426) مبحوثاً من الجمهور العام في هولندا.

وتوصلت نتائج الدراسة إلى أن الأشخاص الذين لديهم المعرفة ذات الصلة، والذين لديهم دافع لحماية أنفسهم، يبلغون عن سلوك أكثر أمانًا على الإنترنت، وأضافت نتائج الدراسة أن الفرصة

التي يتمتع بها الأشخاص لحماية أنفسهم من الهجمات السيبرانية مرتبطة جزئيًا فقط بسلوك الأمن السيبراني لديهم وكيفية تصرفهم معها[14].

ولرصد وتحليل وتفسير استراتيجيات خطاب صحافة التكنولوجيا العربية في كل من مصر والسعودية تجاه الأمن السيبراني، من خلال تحليل آليات خطابات أبواب التكنولوجيا في الموقع الإلكتروني لصحيفتي "اليوم السابع" المصرية و"عكاظ" السعودية، ومحددات تشكيل تلك الآليات، وكذلك العوامل والمتغيرات المؤثرة في إنتاج هذا الخطاب الصحفي سواء عوامل ومتغيرات مجتمعية، أو عوامل ومتغيرات لها علاقة بالمناخ الصحفي والإعلامي المنتج له، جاءت دراسة **(أسماء أحمد أبو زيد، 2021)**، والتي توصلت نتائجها من خلال دراسة تحليلية لخطابات صفحات التكنولوجيا بصحيفة "اليوم السابع" المصرية، وصحيفة "عكاظ" السعودية خلال فترة الدراسة من يناير 2018م إلى يناير2019م، إلى أنه على مستوى أطروحات خطاب صحافة التكنولوجيا العربية محل الدراسة والحجج الداعمة لها إزاء الأمن السيبراني: اتفق خطاب صحافة التكنولوجيا العربية محل الدراسة على أن الحاجة للأمن السيبراني هي حاجة دفاعية عن الذات والمنجزات الوطنية، فلم تعد الهجمات السيبرانية نتاج عمل أشخاص بمفردها أو مجموعات من القراصنة فقط ولكنها أصبحت تضم متخصصين في الجرائم السيبرانية يتعاونون معا ويستثمرون أموال ضخمة فيها، فضلا عن المعرفة والخبرة والمثابرة، وأصبحت قدرات هؤلاء المتخصصين تعادل إن لم تكن أفضل من قدرات الجهات الفاعلة في الدولة، كما وظف خطاب صحافة التكنولوجيا العربية محل الدراسة أسلوب تقديم الأدلة والشواهد، ووضوح الأهداف، ولإبراز استعداد كل من مصر والسعودية لمواجهة الأخطار السيبرانية، وبرزت الاستمالات العقلانية في توظيف خطاب صحافة التكنولوجيا العربية محل الدراسة بشكل رئيس.

كما أوضحت نتائج الدراسة التي تنتمي إلى الدراسات الوصفية التحليلية التفسيرية المقارنة، حيث استخدمت منهج المسح والمنهج المقارن، واعتمدت في بنائها النظري على نظرية المسئولية الاجتماعية لوسائل الإعلام. إلى أن خطاب صحافة التكنولوجيا العربية محل الدراسة اعتمد على آليتين رئيسيتين عند تناوله للأمن السيبراني، وهي: آلية المسئولية، وآلية الكشف والتنوير، للتأكيد على اهتمام الحكومة المصرية والسعودية بملف الأمن السيبراني، واستعدادهما لوقف الهجمات السيبرانية ووضع تصورات مستقبلية لتطور الجريمة الإلكترونية، ووقف مخاطرها على المجتمع[15].

وحول التعرف على اتجاهات النخبة المصرية نحو توظيف الإعلام الأمني لتطبيقات الذكاء الاصطناعي في مكافحة الجرائم الالكترونية ودعم وتعزيز الأمن السيبراني في مصر، وكذلك تقييم النخبة لدور التطبيقات الذكية في إنتاج المحتوى الأمني، مروراً بآليات التوظيف والتأثيرات الإيجابية والسلبية والتحديات والمشكلات ومقترحات التوظيف وذلك في ضوء المعايير المهنية والأخلاقية للإعلام الجديد، جاءت دراسة **(مجدي الداغر، 2021)**، والتي توصلت نتائجها من خلال اعتمادها على منهج المسح وأداة الاستبيان بالتطبيق على عينة عمدية قوامها (106) مفردة موزعة على النخبة "الإعلامية والأمنية والأكاديمية"، إلى اتفاق النخبة المصرية على تنوع الوسائط المتعددة التي سوف تعتمد عليها تطبيقات الذكاء

الاصطناعي عند إنتاج محتواها الأمني، وتصدرت صحافة البيانات أكثر تطبيقات الإعلام الجديد استفادة منها، يليها صحافة الفيديو، والموبيل، وصحافة الدرون.

كما كشفت النتائج اتفاق اتجاهات النخبة نحو مجالات توظيف الإعلام الأمني لتطبيقات الذكاء الاصطناعي في إنتاج المحتوى، وأن التوظيف سوف ينعكس أكثر على تطوير أساليب المعالجة وتنوعها، وهو ما يقلل من جهد الإعلاميين في التغطية الحية والتوجه نحو الإبداع وتطوير المحتوى، والتأكيد على إمكانية استخدام تطبيقات الإعلام الأمني في دراسة وتحليل حجم كبير من المعلومات والبيانات والتعرف على أبعاد الجرائم الالكترونية وتأثيراتها السلبية على أمن المجتمع[16].

المحور الثاني: دراسات تناولت انتهاك الخصوصية عبر تطبيقات ومنصات الإعلام الجديد

تعددت الدراسات الإعلامية التي استهدفت البحث في مشكلة اختراق الخصوصية للمستخدمين للمنصات والتطبيقات الرقمية عبر شبكة الانترنت، ومن ذلك **دراسة (Jose Niño Sales، 2024)**، والتي استهدفت تحليل وتفسير وفهم كيفية تأثير العوامل الديموغرافية للطلاب وتجاربهم على موقفهم وإدراكهم ووعيهم تجاه الخصوصية الشخصية والأمن السيبراني عند استخدامهم لوسائل التواصل الاجتماعي وتحديد ما إذا كانت هناك تصورات لديهم عن حماية معلوماتهم وبياناتهم على حساباتهم على هذه المواقع، وكشفت نتائجها أن الطلاب لديهم موقف إيجابي تجاه استخدام وسائل التواصل الاجتماعي ويشعرون بالثقة مع مقدمي وسائل التواصل الاجتماعي، وأكد المبحوثين على وعيهم بكيفية حماية خصوصيتهم الشخصية والاستفادة من ميزات الأمن السيبراني المتاحة لحساباتهم على وسائل التواصل الاجتماعي.

ومن خلال استخدام الدراسة المنهج الوصفي واعتمادها على التحليل الكمي للبيانات، وتطبيق استمارة استبيان الكتروني على عينة مكونة من (384) مبحوثا من طلاب المراحل التعليمية المختلفة بالفلبين من الابتدائي وحتى الجامعة، توصلت نتائجها إلى وجود اختلافات كبيرة في مستوى وعي الطلاب فيما يتعلق بالخصوصية الشخصية والأمن بين الفئة العمرية والمستوى التعليمي، حيث يحصل الأشخاص ذوو المستوى التعليمي العالي والأكبر سناً عن مستوى أعلى من الوعي عند استخدام وسائل التواصل الاجتماعي عندما يتعلق الأمر بالخصوصية الشخصية والأمن السيبراني[17].

توفي ذات السياق استهدفت **دراسة (ريم المرموم، 2024)**، تقييم نظرة طلبة جامعة الشارقة لمسألة الخصوصية على وسائل التواصل الاجتماعي، استخدمت هذه الدراسة المنهج الكمي، أكمل 146 طالبًا طوعًا استبيانًا إلكترونيا باللغة الإنجليزية، وكشفت النتائج أن 91% من الطلاب كانوا نشطون على منصات التواصل الاجتماعي، ويعد سناب شات وإنستغرام الاختيارين الأكثر تداولاً، ومع ذلك، كان من المثير للمخاوف والقلق أن 92 % من إجمال الطلاب التي أجريت عليهم الدراسة لا يفهمون بشكل كامل ولا يطلعون إطلاقاً على شروط وأحكام هذه المنصات، مما يشير إلى وجود فجوة في الوعي، وعدم إدراك تام لما تترتب عليه الموافقات والقبول التي يتم النقر عليها للتسجيل، وأضافت النتائج أن الكثير من الطلاب لديهم

شكوك ومخاوف من احتمالية انتهاك الخصوصية، حيث احتلت سرقة الهوية المرتبة الأولى في قائمة المخاوف أو استغلالها بأي شكل من الأشكال، ويعد الإطار القانوني الصارم في الإمارات العربية المتحدة الذي يفرض السجن والغرامة على الجرائم الإلكترونية عاملا دفاعيا، تؤكد هذه الدراسة أن زيادة الوعي والمعرفة الرقمية بين الطلاب يعد جانبًا مهمًا يجب أخذه بعين الاعتبار، وأن التدقيق في هذا المجال أمر ضروري[18].

كما استهدفت **دراسة (زينب عبد العظيم عبد الواحد 2023)**، التعرف على استخدام المراهقين لشبكة الفيس بوك وعلاقته بقلق الابتزاز الالكتروني لديهم، وتعد هذه الدراسة من الدراسات الوصفية، واستخدمت منهج المسح، وأداة الاستبيان في جمع البيانات والمعلومات وطبقت الدراسة على عينة عشوائية قوامها (550) مفردة من المراهقين، طلاب "المرحلة الثانوية" بمحافظة المنيا بواقع "275 ذكورًا"، و"275 إناثًا".

وتوصلت نتائجها إلى وجود علاقة ارتباطية طردية ذات دلالة إحصائية بين معدل استخدام المراهقين لشبكة الفيس بوك وقلق الابتزاز الإلكتروني لديهم، وأن غالبية أفراد العينة تعرضوا بالفعل للابتزاز الالكتروني عبر شبكة الفيس بوك وذلك بنسبة تزيد عن 84%، وأن السبب الرئيس والأول من وجهة نظر أفراد العينة نحو حدوث الابتزاز الالكتروني عبر موقع التواصل الاجتماعي "فيس بوك" هو غياب التوعية وضعف الوازع الأخلاقي، وأشارت النتائج أن أكثر أنواع الابتزاز الالكتروني انتشارا من بين الجرائم التي يتم ارتكابها عبر هذا الموقع هي انتحال الشخصية وسرقة الهوية[19].

وللتعرف على دور مواقع التواصل الاجتماعي في التوعية بمخاطر الابتزاز الالكتروني لدى الشباب الجامعي المصري، والتعرف على مدى وعي الشباب بكيفية التعامل مع مواقف الابتزاز الالكتروني التي يتم تناولها عبر مواقع التواصل الاجتماعي، جاءت **دراسة (ياسمين كمال وآخرون، 2023)**، وتوصلت إلى أن نسبة (49%) من الشباب الجامعيين يستخدمون مواقع التواصل الاجتماعي بصفة دائمة، وأن نسبة 26% من عينة الدراسة تعرضت للابتزاز الالكتروني عبر مواقع التواصل الاجتماعي.

ومن خلال اعتماد الدراسة على منهج المسح بالعينة، وتطبيق استبيان على عينة من الشباب الجامعيين بالجامعات المصرية الحكومية (جامعة القاهرة ، جامعة المنيا، جامعة أسيوط)، بلغت 400 مفردة، كشفت الدراسة أنه لا توجد علاقة ارتباط ذات دلالة إحصائية بين معدل استخدام الشباب الجامعي لمواقع التواصل الاجتماعي والتعرض للابتزاز الالكتروني، كما أنه لا توجد فروق ذات دلالة إحصائية بين استجابات الطلاب عن التعرض للابتزاز الإلكتروني تعزى لكل من النوع (ذكور/ إناث) ومتغير المنطقة (وجه بحري/ وجه قبلي)، كما توجد فروق ذات دلالة إحصائية بين استجابات الطلاب عينة الدراسة على مقياس الوعي بمخاطر الابتزاز الإلكتروني تعزى لمتغير النوع (ذكور/ إناث)[20].

وحول هذا الجانب استهدفت دراسة **(Jessica،Rocheleau ،2023)** التعرف على مخاوف المراهقين المصابين بالتوحد فيما يتعلق بحماية بياناتهم الشخصية والأمان على مواقع التواصل الاجتماعي، ومقارنتهم بأقرانهم غير المصابين، لتقييم مواقفهم وسلوكياتهم المتعلق

بالخصوصية والحماية عبر وسائل التواصل الاجتماعي، وقد تم إجراء الدراسة على عينة قدرها (26) مفردة، مقسمة بين (12) مفردة من المراهقين المصابين بالتوحد، و (16) مفردة من غير المصابين بكندا، من خلال مقابلات شبه منتظمة.

وتوصلت نتائج الدراسة إلى أن أفراد عينة الدراسة من المراهقين المصابين بمرض التوحد أكثر كرهاً للمخاطر المتعلقة بحماية البيانات وتعرضها للاختراق عبر وسائل التواصل الاجتماعي، من غيرهم المراهقين غير المصابين بالتوحد، وكشفت نتائج الدراسة أن ذلك ربما يرتبط بعنصر التصميم لهذه المواقع والذي قد تجعل المصابين بالتوحد أكثر عرضة من غيرهم للتنمر والسخرية[21].

كما استهدفت **دراسة (Thilini B. G. Herath 2022)**، التعرف على العوامل التي تؤثر على وعي وإدراك مستخدمي منصات التواصل الاجتماعي المختلفة بالمميزات والخصائص المتعلقة بالأمن والحفاظ على بياناتهم ومعلوماتهم، وتصرفاتهم وسلوكياتهم نحو هذه المميزات.

وأظهرت نتائج الدراسة أن هناك العديد من التهديدات السيبرانية الموجودة داخل منصات التواصل الاجتماعي مثل اختراق الخصوصية، وفقدان الإنتاجية، والتنمر الإلكتروني، والمطاردة عبر الإنترنت والحمل الزائد على المعلومات الاجتماعية، والضرر بالسمعة الشخصية، والبرامج الضارة، والوصول غير المصرح به إلى حسابات وسائل التواصل الاجتماعي للمستخدمين، كما كشفت الدراسة أيضا أن العوامل الديموغرافية، مثل العمر والجنس والمستوى التعليمي، قد لا تكون كذلك بالضرورة عوامل مؤثرة على الوعي السيبراني لمستخدمي الإنترنت[22].

وللتعرف على مدى إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق " الديب فيك" وعلاقته باستخدامهم الآمن لتلك المواقع، وذلك من خلال قياس عدة متغيرات منها إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق، والكشف عن مستوى الاستخدام الآمن لمستخدمي هذه المواقع، وتحديد مستوى ثقة المستخدمين في قدرتهم على كشف التزييف العميق " الثقة المزيفة " وتوضيح الفروق في مستوى إدراك المستخدمين لتهديدات التزييف العميق وفقا للمتغيرات الديموجرافية (النوع، العمر، المستوى التعليمي)، جاءت **دراسة (ولاء محروس، ياسر الناغي، 2022)**، وتوصلت نتائجها إلى وجود علاقة ارتباطية ذات دلالة إحصائية بين مستوى إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق وبيم مستوى استخدامهم الآمن لتلك المواقع، توجد علاقة ارتباطية ذات دلالة إحصائية بين مستوى ثقة مستخدمي مواقع التواصل الاجتماعي في قدرتهم على كشف التزييف العميق وبين مستوى استخدامهم الآمن لتلك المواقع،

كما كشفت نتائج الدراسة التي تنمي إلى حقل الدراسات الوصفية، واعتمدت على منهج المسح الإعلامي، وتم تطبيق استمارة الاستبيان الالكتروني على عينة قوامها 600 مفردة من مستخدمي مواقع التواصل الاجتماعي، إلى وجود فروق ذات دلالة إحصائية في مستوى إدراك مستخدمي مواقع لتواص الاجتماعي لتهديدات التزييف العميق وفقا لمتغيرات (النطاق الجغرافي، النوع، المستوى التعليمي)[23].

كما استهدفت **دراسة (Sophie C. Boerman ، 2022)**، التعرف على كيفية تفعيل المبحوثين من الجمهور الهولندي لخصائص حماية بياناتهم الشخصية عبر استخدامهم لشبكة الانترنت والتطبيقات المرتبطة بها، وكيفية إدارة حمايتهم الشخصية، وقد تمت الدراسة من خلال نظرية دافع الحماية، للتحقق من سلوك المستخدمين اتجاه حماية خصوصيتهم عبر الشبكة العنبكوتية، وقد تم إجراء دراسة ميدانية من خلال استبيان تم توزيعه على مرحلتين خلال عامين منفصلين (2016 ، 2017)، وتم تطبيقه على عينة مكنة من (928) مفردة.

وتوصلت النتائج إلى المبحوثين عينة الدراسة لا يهتمون كثيراً بحماية بياناتهم الشخصية عبر شبكة الانترنت، وأنهم بالرغم من ثقتهم في تدابير الحماية المتاحة لهم، إلا أنهم لا يثقون كثيرا في فعاليتها في حماية بياناتهم ومعلوماتهم الشخصية، وأضافت النتائج أن هناك علاقة ارتباطية بين سلوك الحماية لدى أفراد العين والشدة المتصورة عن الآثار السلبية الناتجة عن اختراق بياناتهم الشخصية[24].

وللتعرف على اتجاهات الشباب الجامعي نحو انتهاك الحياة الخاصة عبر شبكات التواصل الاجتماعي وآليات حماية الخصوصية، وعرضت الدراسة إطارا منهجيا تضمن على مجموعة مصطلحات وهي (انتهاك الخصوصية، الخصوصية الرقمية، الحياة الخاصة، شبكات التواصل الاجتماعي)، كشفت نتائج **دراسة (هاني إبراهيم محمد، 2022)**، أن معظم أفراد العينة يرون أن مواقع التواصل الاجتماعي تقوم باختراق الخصوصية لمستخدميها، لكنهم لا يوافقون على اختراق خصوصياتهم حتى وإن كانت لأغراض إعلانية، وأوضحت الدراسة ارتفاع وعي أفراد العينة بأن استخدام معلوماتهم الشخصية من قبل أي شخص هو جريمة الكترونية يعاقب عليها القانون، كما يتوفر لدى العينة دراية بكيفية حماية بياناتهم الشخصية.

وأضافت الدراسة التي اعتمدت على منهج المسح الميداني، واختيرت عينتها بالطريقة العشوائية البسيطة وكان قوامها (300) مفردة من الشباب الجامعي مستخدمي شبكات التواصل الاجتماعي، وذلك خلال شهري أكتوبر ونوفمبر (2021 م)، واشتملت الأدوات على صحيفة استقصاء الكترونية، بوجود علاقة ارتباطية ذات دلالة إحصائية بين اتجاهات الشباب الجامعي نحو انتهاك الحياة الخاصة عبر الشبكات الاجتماعية وبين وعيهم بآليات حماية الخصوصية، كما أكدت على وجود علاقة ارتباطية ذات دلالة إحصائية بين دوافع تعرض الشباب الجامعي للشبكات الاجتماعية وبين اتجاهاتهم نحو انتهاك الحياة الخاصة عبر الشبكات الاجتماعية، وأوصت الدراسة بأهمية التأكيد على ضرورة تقديم مضامين توعوية للشباب بأشكال انتهاك الخصوصية والموقف القانوني لتلك الانتهاكات[25].

وفي السياق ذاته استهدفت **دراسة (Ralf De Wolf، 2020)** رصد إدارة خصوصية المراهقين لبياناتهم الخصوصية عبر مواقع التواصل الاجتماعي، وطيف يتحكمون بشكل فردي في هذه المعلومات والبيانات الشخصية، في إطار نظرية إدارة خصوصية الاتصالات، وتم تطبيق الدراسة من خلال استبيان تم توزيعه على (2000) مفردة من المراهقين في بلجيكا.

وتوصلت الدراسة إلى أن التحكم الفردي في المعلومات والبيانات الشخصية من جانب المراهقين عبر حساباتهم في مواقع التواصل الاجتماعي في حد ذاته أمر مرغوب فيه ولكنه

غير كافٍ، مما يعطي مفهوماً محدوداً للتعرف على ممارسات خصوصية المراهقين، لذا يجب التركيز على إدارة الخصوصية الشخصية والتفاعلية لفهم ممارسات حقيقية لخصوصية المراهقين في النهاية، كما أن المراهقين يهتمون بدرجة أقل بحامية خصوصياتهم من البيانات والمعلومات الشخصية عند تبادلها مع الأصدقاء[26].

التعليق على الدراسات السابقة:

من خلال الرصد السابق للدراسات ذات الصلة بالدراسة الحالية ومتغيراتها، وتقديم عرضاً مفصلاً عنها سواء الدراسات العربية أو الأجنبية، يمكن تقديم عدد من التعليقات كما يلي:

من حيث الموضوع أو الهدف: تنوعت أهداف الدراسات السابقة سواء التي تناولت الأمن السيبراني، أو انتهاك الخصوصية عبر تطبيقات ومنصات الإعلام الجديد، فسعى بعضها إلى الكشف عن كيفية تأثير معرفة الجمهور بالأمن السيبراني، والتصور الذاتي لديهم على قضايا الوعي بالأمن السيبراني، مثل دراسة (Mrittika Rani، 2024)، ودراسة (Mengqi Liao، 2023)، ودراسة (Jose Niño Sales،2024)، واستهدفت أخرى تقييم معرفة مستخدمي مواقع التواصل الاجتماعي لحماية بياناتهم الشخصية، وآليات ذلك، مثل دراسة (ريم المرموم، 2024)، ودراسة (Rocheleau، Jessica ، 2023)، وسعت دراسات أخرى لتحديد دور وسائل الإعلام في تعزيز الأمن السيبراني، ورفع مستوى وعي الجمهور بمخاطر انتهاك الخصوصية، مثل دراسة (شيرين عبد الحفيظ، 2023)، ودراسة (Thilini B. G. Herath، 2022).

من حيث نوع الدراسة والمناهج البحثية: انتمت أغلب الدراسات السابقة التي تناولت الأمن السيبراني، وانتهاك الخصوصية الرقمية للمستخدمين لشبكة الانترنت ومنصاتها المختلفة، إلى نوع الدراسات الوصفية، مثل دراسة (مطلق سعد العميري، 2024)، ودراسة (Mengqi Liao، 2023)، ودراسة (ولاء محروس، ياسر الناغي، 2022)، واستخدم الكثير منها منهج المسح، مثل دراسة (هدير محمود، 2023)، ودراسة (زينب عبد العظيم عبد الواحد 2023)، ودراسة (Jose Niño Sales،2024)، ودراسة Kleij، (R. van der ، 2021).

من حيث الأطر والمداخل النظرية: تعددت الأطر والمداخل النظرية التي اعتمدت عليها الدراسات السابقة في المحورين السابقين، فقد استخدمت (شيرين عبد الحفيظ، 2023)، نظرية انتشار المستحدثات، واستخدمت دراسة (Sophie C. Boerman ، 2022)، نظرية دافع الحماية، واعتمدت دراسة (أسماء أحمد أبو زيد، 2021)، على نظرية المسئولية الاجتماعية لوسائل الإعلام، واستخدمت دراسة (Ralf De Wolf، 202K) نظرية إدارة خصوصية الاتصالات.

من حيث أدوات جمع البيانات والعينة: تباينت الأدوات البحثية والعينات التي اعتمدت عليها الدراسات السابقة، وذلك بناء على طبيعة الدراسة والأهداف التي تسعى لتحقيقها، فبعضها دراسات ميدانية قامت بتطبيق استبيان على عينة من الجمهور مثل دراسة(مطلق سعد العميري، 2024)، ودراسة (Anakha Prakash، 2024)، ودراسة (Mengqi Liao،

2023)، والبعض الأخر دمج بين الدراسات التحليلية والميدانية مثل دراسة(Anakha Prakash، 2024)، ودراسة (أماني حمدي ، إيمان عبد المنعم، 2022).

من حيث النتائج: توصلت الدراسات السابقة إلى العديد من النتائج، حيث أكد بعضها على أهمية الأمن السيبراني مثل دراسة (Mrittika Rani، 2024)، وبعضها توصلت إلى أهمية رفع وعي الجمهور بالمخاطر المحتملة لانتهاك الخصوصية، مثل دراسة (Anakha Prakash، 2024)، ودراسة (شيرين عبد الحفيظ، 2023)، وبعضها كشف عن اختلاف مستوى الوعي لدى الفئات المختلفة من الجمهور، وتأثير الوامل الديموغرافية على ذلك، مثل دراسة (Jose Niño Sales،2024)، ودراسة (Mengqi Liao، 2023)، ودراسات أخرى كشفت عن عدم ثقة المستخدمين لآليات الحماية داخل المنصات والتطبيقات الرقمية عبر شبكة الانترنت، وأنها قد تخترق بياناتهم مثل (Sophie C. Boerman، 2022)، ودراسة (هاني إبراهيم محمد، 2022).

كما أمكن الاستفادة من مراجعة الدراسات السابقة فيما يلي:

- بلورة المشكلة البحثية، ومعرفة الجوانب الجديدة لدراستها.
- تحديد أهداف الدراسة بدقة، وتحديد تساؤلاتها.
- تحديد المنهج العلمي المناسب للدراسة الحالية، وهو منهج المسح.
- تحديد الأدوات البحثية لجمع البيانات، وكيفية تحديد حجم العينة.

تساؤلات الدراسة:

- ما مستوى معرفة الشباب الكويتي بالأمن السيبراني؟
- إلي مدى يحرص الشباب الكويتي على تأمين وحماية بياناتهم الشخصية عبر تطبيقات ومنصات الإعلام الجديد التي يستخدمونها؟
- أي من التطبيقات الالكترونية الأكثر استخداما من جانب الشباب الكويتي، ومدى ثقتهم فيها؟
- كيف يتعامل الشباب الكويتي مع هجمات القرصنة الإلكترونية حال تعرضهم لها؟
- ما اتجاهات الشباب الكويتي نحو السلوكيات التي يتبعونها للحفاظ على بياناتهم من السرقة وانتهاك الخصوصية عبر تطبيقات ومنصات الإعلام الجديد؟
- ما اتجاهات الشباب الكويتي نحو الأسباب المؤدية لانتشار جرائم انتهاك الخصوصية عبر تطبيقات ومنصات الإعلام الجديد؟
- ما اتجاهات الشباب الكويتي نحو الأضرار والآثار السلبية لمخاطر انتهاك الخصوصية على مستوى الأفراد والمجتمعات؟
- كيف يمكن توعية الشباب الكويتي بمخاطر انتهاك الخصوصية عبر شبكة الانترنت؟

نوع الدراسة:

تنتمي هذه الدراسة إلى حقل البحوث الوصفية Descriptive Studies التي تستهدف تقرير خصائص الظاهرة، وتعتمد على جمع الحقائق وتحليلها وتفسيرها لاستخلاص دلالتها، للوصول إلى نتائج تقبل التعميم.

والظاهرة التي تسعى الدراسة الحالية إلى تقرير خصائصها هي: " اتجاهات الشباب الكويتي نحو أهمية الأمن السيبرانى.. في ضوء مخاطر انتهاك الخصوصية عبر تطبيقات ومنصات الإعلام الجديد " وذلك بهدف الوصول إلى نتائج يمكن تعميمها والاستفادة منها.

منهج الدراسة:

نظراً لأن طبيعة الدراسة تهدف إلى وصف وتحليل الظاهرة الإعلامية من مختلف جوانبها فإن هذه الدراسة تعتمد على منهج المسح "Survey Method " وفي إطار ذلك تعتمد الدراسة على أسلوب المسح بالعينة وذلك فيما يتعلق بالشباب الكويتي" عينة الدراسة".

مجتمع الدراسة:

يتمثل مجتمع الدراسة في الشباب الكويتي الذين تزيد أعمارهم عن 18 عاماً، ويستخدمون التطبيقات والمنصات الإلكترونية عبر شبكة الإنترنت.

عينة الدراسة:

تم اختيار العينة بطريقة عمدية غرضية متاحة مكونة من 400 مفردة من الشباب الكويتي دون التمييز بين الذكور والإناث بإعطائهم الفرصة المتكافئة نفسها للاختيار، ويوضح الجدول التالي خصائص عينة الدراسة.

جدول رقم(1) يوضح البيانات الديموغرافية للمبحوثين:

الخصائص	الفئات	ك	%
النوع	ذكر	273	68.25
	أنثى	127	31.75
	المجموع	400	100.00
مستوى التعليم	متوسط	99	24.75
	جامعي	252	63.00
	فوق الجامعي (ماجستير- دكتوراه)	49	12.25
	المجموع	400	100.00

العمر	من 18 إلى أقل من 20 عام	105	26.25
	من 20 إلى أقل من 25 عام	109	27.25
	من 25 إلى أقل من 35عام	186	46.50
	المجموع	400	100.00
الحالة الاجتماعية	أعزب	147	36.75
	متزوج	238	59.50
	مطلق	12	3.00
	أرمل	3	0.75
	المجموع	400	100.00
المستوى الاقتصادي	منخفض	63	15.75
	متوسط	223	55.75
	مرتفع	114	28.50
	المجموع	400	100.00

أدوات جمع البيانات:

استمارة الاستبيان:

اعتمدت الدراسة على استمارة الاستبيان، لتطبيقها على عينة من الشباب الكويتي، ويعد الاستبيان أحد الأساليب المستخدمة في جمع بيانات أولية وأساسية مباشرة من العينة المختارة أو من جميع مفردات البحث عن طريق توجيه مجموعة من الأسئلة المحددة والمعدة مقدماً[27].

إجراءات الصدق والثبات:

أولاً: اختبار الصدق.

قام الباحث بإجراء اختبار الصدق لاستمارة الاستبيان، حيث تم عرضها على مجموعة من المحكمين من أساتذة الإعلام والمتخصصين في البحث العلمي، للحكم عليها والتأكد من صدقها وصلاحيتها لتحقيق أهداف الدراسة والإجابة على التساؤلات، وتم تعديلها بناء على الملاحظات التي أبدوها، حيث تم حذف بعض الأسئلة المكررة، واستبعاد الأسئلة التي تحمل تناقضاً، وإضافة أخرى[28].

ثانياً: اختبار الثبات.

تم إجراء اختبار الثبات لاستمارة الاستبيان من خلال أسلوب إعادة الاختبار على عينة قوامها 40 مفردة بواقع 10% من العينة، وذلك بعد خمسة عشر يوماً من إجابتهم على الاستمارة الأولى، وبمقارنة إجابات كل مبحوث في المرتين الأولى والثانية وحساب المتوسط العام لمعدلات الاتساق تبين أن هذه الاستمارة ذات مستوى ثبات قدره 91%، وهي نسبة تشير إلى ثبات الاستمارة وقابليتها للتطبيق.

المعالجة الإحصائية للبيانات:

بعد الانتهاء من جمع بيانات الدراسة، قام الباحث بترميز البيانات وإدخالها إلى الحاسب الآلي، ثم معالجتها وتحليلها واستخراج النتائج الإحصائية وذلك باستخدام برنامج "الحزمة الإحصائية للعلوم الاجتماعية "Statistical Package for Social Science) "SPSS). وبناء عليه تم عمل مقاييس وصفية تشمل الجداول والتوزيعات التكرارية، والمقاييس التجميعية، وتطبيق المعاملات الإحصائية التي تلائم كل متغير من متغيرات الدراسة وفق الآتي:

- التكرارات البسيطة. Frequency والنسب المئوية Percent.
- المتوسط الحسابي Mean. والانحراف المعياري Std. Deviation.
- الأوزان النسبية: وذلك عن طريق حساب المتوسط الحسابي لمقياس ليكرت الثلاثي ثم ضرب النتائج × 100، ثم قسمة النتائج على الحد الأقصى لدرجات المقياس
- معامل ارتباط بيرسون (Pearson Correlation) لدراسة شدة واتجاه العلاقة الارتباطية بين متغيرين من مستوي المسافة أو النسبة. وقد اعتبرت العلاقة ضعيفة إذا كانت قيمة المعامل أقل من 0.300، ومتوسطة إذا كانت ما بين 0.300: 0.600، وقوية إذا كانت أكثر من 0.600.
- اختبار (Independent Samples T Test) لمقارنة متوسطي عينتين مستقلتين والمعروف اختصارا باختبار "ت" أو (T- Test).
- اختبار تحليل التباين في اتجاه واحد (One Way ANOVA) والمعروف اختصارا ANOVA، أو اختبار "ف" وذلك لقياس الفروق بين المتوسطات بين أكثر من مجموعتين.
- الاختبارات البعدية (Post Hoc Tests) بطريقة أقل فرق معنوي (Least Significance Difference) والمعروف اختصارا باسم (LSD) لمعرفة مصدر الفروق والتباين وإجراء المقارنات الثنائية بين المجموعات التي يثبت اختبار (ANOVA) وجود فروق دالة إحصائيا بينها.

مستوى الدلالة المعتمد في هذه الدراسة:

سيعتمد الباحث على مستوى دلالة يبلغ 0.05، لاعتبار الفروق ذات دلالة إحصائية من عدمه، وبناء على ذلك سيتم قبول نتائج الاختبارات الإحصائية عند درجة ثقة 95% فأكثر، أي عند مستوى معنوية 0.05 فأقل.

فروض الدراسة:

الفرض الأول: توجد علاقة ارتباطية ذات دلالة إحصائية بين مستوى حرص المبحوثين عينة الدراسة على تأمين وحماية بياناتهم الشخصية من الانتهاك، وبين اتجاههم نحو سلوكياتهم في الحفاظ عليها.

الفرض الثاني: توجد علاقة ارتباطية ذات دلالة إحصائية بين سلوكيات المبحوثين لتأمين ولحماية بياناتهم الشخصية من الانتهاك والأضرار، واتجاههم نحو الآثار السلبية لمخاطر انتهاك الخصوصية على مستوى الفرد والمجتمع.

الفرض الثالث: توجد علاقة ارتباطية ذات دلالة إحصائية بين ثقة المبحوثين عينة الدراسة في حماية بياناتهم الشخصية عبر تطبيقات الإعلام الجديد التي يستخدمونها، وبين سلوكياتهم في الحفاظ عليها.

الفرض الرابع: توجد علاقة ذات دلالة إحصائية بين كثافة استخدام المبحوثين عينة الدراسة لمنصات وتطبيقات الإعلام الجديد، وبين مستوى حرصهم على حماية بياناتهم من الاختراق.

الفرض الخامس: توجد فروق ذات دلالة إحصائية بين المبحوثين عينة الدراسة في اتجاههم نحو مفهوم الأمن السيبراني وانتهاكات الخصوصية، وبين متغيراتهم الديموغرافية (النوع - السن- المستوى التعليمي- الحالة الاجتماعية - المستوى الاقتصادي).

الفرض السادس: توجد فروق ذات دلالة إحصائية بين المبحوثين عينة الدراسة في اتجاههم نحو الأضرار والآثار السلبية لمخاطر انتهاك الخصوصية على مستوى الفرد والمجتمع، وفقاً لمتغيراتهم الديموغرافية (النوع- السن- المستوى التعليمي- الحالة الاجتماعية- المستوى الاقتصادي).

الإطار النظري للدراسة:

نظرية إدارة خصوصية الاتصالات " Communication Privacy Management "Theory (CPM).

ترتكز هذه الدراسة على نظرية إدارة الخصوصية الشبكية، والتي صاغتها (Sandra Petronio)، وتقوم على إتباع نهج قائم على إدارة قواعد لكشف عن المعلومات التي تخص المستخدمين والتحكم فيها، وأن نشر البيانات الشخصية، أو التعبير عن مشاعرنا الخاصة أمام الجميع هو أمر محفوف بالمخاطر، ويشعرنا بعد الارتياح، وذلك يرتبط بكون الفرد يشعر بأنه المالك الشرعي للمعلومات الخاصة به، لذا لا يجوز لأحد أن يطلع عليها بدون رغبته، ويمكن أن تشمل مخاطر الإفصاح عن البيانات الشخصية على: الكشف عن المعلومات الخاصة لشخص خطأ، أو الكشف عنها في وقت غير مناسب، أو إخبار الكثيرين عن أنفسنا، أو تعريض الآخرين للخطر، لذا تفترض نظرية غدارة الخصوصية الشبكية(الاتصالات) أن الأشخاص يتخذون خيارات بشأن الكشف أو الإخفاء بناء على معايير وشروط يعتقدون بها، بما يشير إلى أن الأشخاص يقعون وسط خيارين متعارضين: الأول، أن الأشخاص لديهم الرغبة في الكشف عن بياناتهم الشخصية بوصفها طريقة لتحقيق هدف ما، والثاني: أن الأشخاص في نفس الوقت يرغبون في المحافظة على خصوصيتهم البيانية والمعلوماتية[29].

حيث تستطيع هذه النظرية تقديم فهم أفضل لأهمية مشاركة المستخدمين لمعلوماتهم الشخصية أو حجبها على منصات الإعلام الجديد، خاصة وأن عملية إدارة الخصوصية ليست عملية فردية خالصة؛ حيث إن مثل هذه المعلومات تكون مشتركة مع أطراف

مختلفة تشارك في العملية الاتصالية، مثل الأصدقاء وأفراد الأسرة والمجتمعات الافتراضية عبر المنصات الرقمية، فعلى سبيل المثال يسمح موقع "تويتر" للعديد من الأفراد لمشاركة وامتلاك المعلومات المختلفة مع الآخرين، ولكن على الجهة الأخرى يتيح للعديد من الأفراد القدرة على السيطرة على خصوصية بياناتهم.

وترى هذه النظرية أن كال طرفي الاتصال سواء الكاشف لمعلوماته أو مستقبل هذه المعلومات، لديهم درجة من الوعي الخاص المرتبط بملكية المعلومات التي تم الإفصاح عنها، خاصة وأن تلك الحدود تم إقرارها عن طريق الطرفين، ولذلك فبمجرد قيام الشخص بالإفصاح عن هذه المعلومات، فالأفراد المستقبلين يقومون برسم الحدود الخاصة بهم، خاصة وأن هذه المعلومات الشخصية أصبحت ملكية مشتركة بينهم، حيث يعتبر الإفصاح عن أي معلومات عبر المنصات الجديدة، اعتراف ضمني بالتخلي طواعية عن درجة من درجات التحكم والملكية في المعلومات الشخصية، وبالتالي فإن الأفراد الذين يلجئون إلى الإفصاح عن معلوماتهم الشخصية أو إخفاءها يتبعون مجموعة من المعايير التي يرون أنها مميزة وتساعدهم على تحقيق هدفهم(30).

ووفقا لذلك فإن الأفراد يستطيعون إدارة المعايير المرتبطة بخصوصية بياناتهم من خال نظام محدد يستطيع أن ينظم كل مراحل عملية الكشف عن المعلومات، ويشمل كيفية تنسيق الحدود بين الأفراد، فالنظرية تشير إلى أن الأفراد لديهم مجموعة محددة من المعايير خاصة فيما يرتبط باتخاذ قرار حول إدارة خصوصيتهم، فالنظرية ترى أن هناك خمس عوامل تؤثر في كيفية تطوير معايير الخصوصية وهي: الثقافة – النوع – الدوافع – السياق – معدل الإيجابيات والخطورة(31).

<u>بالإضافة إلى العوامل السابقة، هناك أيضا ست فرضيات تساعد على تفسير كيفية إدارة الأفراد لخصوصية بياناتهم وهي(32):</u>

- الأفراد يدركون أن المعلومات الشخصية في المنصات الافتراضية هي ملك لهم .
- الأفراد لديهم اقتناع أن لهم القدرة على التحكم في تدفق المعلومات.
- الأفراد يقومون بتطوير واستخدام قواعد معينة خاصة بالخصوصية وفقا إلى مجموعة من المعايير الهامة بالنسبة لهم من أجل التحكم في بياناتهم ومعلوماتهم.
- عندما يعطي الأفراد إمكانية الوصول إلى معلوماتهم الشخصية إلى أشخاص آخرين، فإنه يتم اعتبار هذا الأمر بمثابة ملكية جماعية يتحمل كافة الأفراد فيه مسئولية هذه المعلومات.
- في عملية الملكية الجماعية، يتم تحديد وتنسيق القواعد الخاصة بالخصوصية مرة أخرى.
- يحدث اضطراب في المعايير الخاصة بالخصوصية عندما يتعرض المستخدم لانتهاكات وأخطاء في إدارة خصوصية معلوماته.

وفي هذا الإطار تم توظيف النظرية في الدراسة الحالية للتعرف على مدى إدراك الشباب الكويتي بخصوصية بياناتهم عبر استخدامهم لتطبيقات ومنصات الإعلام الجديد المختلفة على شبكة الإنترنت، ومستوى حرصهم على تأمين وحماية بياناتهم الشخصية من التعرض لانتهاكات الخصوصية، وكيف يقومن بحمايتها.

الإطار المعرفي للدراسة:

مفهوم الأمن السيبراني:

عرف التقرير الصادر عن الاتحاد الدولي للاتصالات عام 2011 الأمن السيبراني بأنه " مجموعة من المهمات مثل" تجميع وسائل وسياسات وإجراءات أمنية، ومبادئ توجيهية، ومقاربات لإدارة المخاطر، وتدريبات، وممارسات فضلى، وتقنيات" يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين(33).

كما أنه عبارة عن مجموعة الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به وسوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني(34).

عناصر الأمن السيبراني:

حتى يتحقق الهدف من الأمن السيبراني، لابد أن تتوفر مجموعة من العناصر مع بعضها البعض ليكتمل الدور، ومن أهم عناصر الأمن السيبراني:

التقنية: تشكل التقنيات التكنولوجية دورا في غاية الأهمية في حياة الأفراد والمنظمات حيث توفر الحماية الفائقة لهم أمام الهجمات السيبرانية وتشمل حماية الأجهزة بمختلف أشكالها الذكية والحاسوبية والشبكات بالاعتماد على جدران الحماية واستخدام برامج مكافحة الفيروسات الضارة وغيرها.

الأشخاص: يستوجب الأمر لزوماً على الأشخاص من مستخدمي البيانات والأنظمة في منشأة ما استخدام مبادئ حماية البيانات الرئيسية كتحديد كلمة مرور قوية وتفادي فتح الروابط الخارجية والمرفقات عبر البريد الإلكتروني إلى جانب القيام بنسخ احتياطي للبيانات.

الأنشطة والعمليات: يتم توظيف الأشخاص والتقنيات للقيام بالعديد من العمليات والأنشطة وتسييرها بما يتماشى مع تطبيق أسس الأمن السيبراني والتصدي لهجماته بكل كفاءة(35) .

أنماط وأشكال التهديدات السيبرانية وانتهاك الخصوصية عبر تطبيقات ومنصات الإعلام الجديد:

يمكن تقسيم التهديدات الرقمية التي تواجه الدول والأفراد على حد سواء إلى أربعة أنواع، كما يلي[36]:

- **هجمات الحرمان من الخدمة:** ويتم فيها إطلاق حزمة كبيرة من الطلبات والمهمات على خوادم الضحية بصورة تفوق قدرة الخادم أو الجهاز على معالجتها والاستجابة لها، مما يؤدي إلى توقفه بشكل جزئي أو كلي أو إبطاء عمله، وهذا ما ينتج عنه ضررا للمستخدم النهائي، وتستعمل هذه الهجمات بكثرة ضد مواقع الانترنت أو البنوك أو المؤسسات بهدف التأثير عليها أو لدفع فدية مالية.
- **إتلاف المعلومات أو تعديلها:** وهي هجمات تستهدف الوصول لمعلومات الضحية عبر شبكة الانترنت أو الشبكات الخاصة، والقيام بعملية تعديل البيانات الهامة دون أن يكتشف الضحية ذلك، فالبيانات تبقى موجودة لكنها مضللة، وقد تؤدي إلى نتائج كارثية خاصة إذا تمثلت البيانات في معلومات أمنية أو مواعيد أو خرائط سرية أو خاصة بالصناعات الحساسة لاسيما الصناعات العسكرية.
- **التجسس على الشبكات:** والمقصود به الدخول غير المصرح والتجسس على شبكات الخصم أو المنافس، دون تدمير أو تغيير في البيانات والمعلومات، والهدف من الهجمة الحصول على معلومات قد تكون تجارية أو خطط تسويقية أو اقتصادية أو مالية أو أسرار حربية أو سياسية، مما يؤثر سلبا على مهام الخصم.
- **تدمير المعلومات:** حيث يتم في هذه الأخيرة مسح وتدمير كامل للأصول والمعلومات والبيانات الموجودة على الشبكة، ويصطلح عليها " تهديد لسلامة المحتوى" ويتمثل في إحداث تغيير في البيانات والمعلومات سواء بالحذف أو التدمير من قبل أشخاص غير مخولين لذلك.

دوافع ارتكاب جرائم انتهاك الخصوصية:

تتنوع وتختلف دوافع ارتكاب جرائم انتهاك الخصوصية عبر تطبيقات ومنصات الإعلام الجديد وذلك وفقاً لنوعها والمستهدف منها ونوع الجاني وذلك على النحو التالي[37]:

- **الدافع السياسي:** ويأتي نتيجة بروز مناطق جديدة للصراع في العالم، وتغير الطبيعة المعلوماتية للدول، حيث أصبح الاعتماد على منصات الانترنت ضرورة، وأصبح الاختراق من أجل الحصول على معلومات سياسية أو اقتصادية مسألة أكثر أهمية للدول والعصابات المنظمة حول العالم، ورغم تزايد جرائم القرصنة وسرقة البيانات والمعلومات، إلا أن هناك تطبيقات ذكية للكشف عن المحتوى المزيف.
- **الدافع التجاري:** تتعرض الشركات الكبرى للمنافسة وأعمال تخريب وقرصنة من شركات أخرى، ويجري هذا العمل بشكل مستمر، خاصة الشركات العاملة في مجال النفط، حيث استهدف أحد برامج الفدية بعض الثغرات في أنظمة التشغيل"

مايكروسوفت " وأصاب ماليين الحاسبات في 150 دولة في مختلف قطاعات المال والأعمال مايو 2017م، وأدى هذا الهجوم السيبراني إلى إصابة ما لا يقل عن 81 منظمة تعمل في الخدمات الصحية، مما ع طل المعدات الطبية عن العمل، وأثر بشكل كبير على صحة وسلامة المرضى.

- **الدافع الفردي:** تأتى محاولات القرصنة والاحتيال الإلكتروني نوعا من التباهي بإختراق أجهزة الغير، ما لبثت أن تحولت تلك الظاهرة إلى اختراق عصابات لمؤسسات وشركات على الانترنت، وتمارس أعمال إرهاب وتخريب ضد دول وشخصيات عامة. كما احترف العديد من الأشخاص تلك الجرائم لاختراق حسابات أشخاص على منصات التواصل الاجتماعي، وتطبيقات الهواتف المحمولة وسرقة بياناتهم الشخصية ومساومتهم عليها ماديا ومعنويا، وإلحاق أضرار بالغة بهم.

آليات حماية الحق في الخصوصية عبر المنصات والتطبيقات الإعلامية الجديدة:

إن حماية الخصوصية في البنية الرقمية عملية وليست إجراء، بمعنى أنها تنطلق من وجهة معينة وهادفة، وهي عبارة عن مجموعة من الوسائل والإجراءات، التي لابد وأن تشمل مجالين: المجال التقني، والمجال القانوني.

حماية الخصوصية في المجال التقني.

لقد اتجهت العديد من الدول إلى وسائل متعددة لحماية الحق في الخصوصية للأفراد في نظام معالجة المعلومات آليا، ومن ضمن ذلك هو إخضاع هذه النظم الآلية لإشراف الدولة وكذلك منع تخزين معلومات معينة عن الأفراد لضوابط معينة .

كذلك تمكين صاحب البريد الإلكتروني أو حساب بشبكة التواصل الاجتماعي من الإطلاع على المعلومات الخاصة به للتأكد من صحتها وإن وجدت أخطاء بإمكانه تصحيحها، وأهم الوسائل المستعملة في هذا المجال هي تقنيات التشفير التي تعد في مقدمة الوسائل المبتكرة في مجال توفير أمن وسلامة وحرية المعلومات والصفقات عبر المنصات الرقمية.

حماية الخصوصية في المجال القانوني.

حيث تولي بعض التشريعات اهتماما خاصا بإقرار إجراءات وقائية حماية للحق في الخصوصية لأن الطبيعة الخاصة بهذه الإجراءات التي يتم بها الاعتداء على الحياة الخاصة على المنصات الرقمية ظاهرة إعلامية جديدة تتميز بسرعة الانتشار والوصول إلى أكبر عدد من الجمهور بأقصر وقت ممكن وبأقل تكلفة، وفي المقابل لذلك فان الإجراءات الوقائية ستهدف في المقام الأول التدخل سريعا لمنع المساس بالحق في الخصوصية[38].

المفاهيم والمصطلحات الإجرائية:

مفهوم الأمن السيبراني: وهو يهتم بأمن المعلومات والبيانات والعمليات التي يتم من خلالها حماية معدات الحاسب والمعلومات والخدمات من أي تدخل غير مشروع، حيث

يتم استخدام مجموعة من وسائل التقنية لمنع الاستخدام غير المصرح به، ومنع سوء استغلال المعلومات الإلكترونية، ونظم الاتصالات والمعلومات التي تحتويها[39].

ويمكن تعريفه إجرائيا بأنه: الممارسات التي تتخذها الدول والمؤسسات والأفراد لحماية الأنظمة والشبكات والبرامج من الهجمات الرقمية، التي تهدف عادةً إلى الوصول إلى المعلومات، أو تغييرها أو إتلافها أو ابتزاز المال من المستخدمين أو مقاطعة العمليات التجارية، وصولا إلى تهديد الأمن القومي للدول.

تعرف" الخصوصية الرقمية" بأنها: وصف لحماية البيانات الشخصية للفرد، والتي يتم نشرها وتداولها من خلال وسائط رقمية، وتتمثل البيانات الشخصية في البريد الإلكتروني، والحسابات البنكية، والصور الشخصية، ومعلومات عن العمل والمسكن وكل البيانات التي نستخدمها في تفاعلنا على الإنترنت أثناء استخدامنا للحاسب الآلي أو التليفون المحمول أو أي من وسائل الاتصال الرقمي بالشبكة العنكبوتية[40].

المفهوم الإجرائي لانتهاك الخصوصية: هو عملية اختراق المعلومات الخاصة بالأفراد أو المؤسسات المستخدمة لشبكة الإنترنت أو أحد تطبيقاتها ومنصاتها المختلفة، والاطلاع على هذه البيانات دون إذن أو موافقة من صاحبها، أو استخدامها بما يضر بمالكها ماديا أو معنوياً.

نتائج الدراسة:

جدول رقم(2) يوضح درجة استخدام المبحوثين لتطبيقات ومنصات الإعلام الجديد عبر شبكة الانترنت

درجة الاستخدام	ك	%	المتوسط الحسابي	الانحراف المعياري
دائماً	291	72.75	2.6875	0.54368
أحياناً	93	23.25		
نادراً	16	4.00		
المجموع	400	100.00		

تشير بيانات الجدول السابق إلى ما يلي:

– أن مستوى استخدام المبحوثين عينة الدراسة للتطبيقات ومنصات الإعلام الجديد المختلفة عبر شبكة الانترنت جاء مرتفعا، بمتوسط حسابي بلغ 2.6875، حيث جاءت نسبة من يستخدمونها بشكل " دائم " بنسبة 72.75%، بينما جاءت نسبة من يستخدمونها " أحياناً " 23.25%، في حين بلغت نسبة من يستخدمونها " نادراً " 4%.

جدول رقم (3)يوضح معدل الاستخدام اليومي للمبحوثين لتطبيقات ومنصات الإعلام الجديد

معدل الاستخدام اليومي	ك	%
من ساعة لأقل من ساعتين	13	3.25
من ساعتين لأقل من 4 ساعات	146	36.50
أكثر من 4 ساعات	241	60.25
المجموع	400	100.00

تشير بيانات الجدول السابق إلى ما يلي:

– أن نسبة من يستخدمون تطبيقات ومنصات الإعلام الجديد المختلفة عبر شبكة الانترنت من المبحوثين عينة الدراسة بمعدل يومي يتراوح بين " ساعة لأقل من ساعتين " بلغت 3.25%، بينما نسبة من يستخدمون هذه التطبيقات بمعدل يومي يتراوح بين " ساعتين لأقل من 4 ساعات " بلغت 36.50%، في حين أن نسبة من يستخدمونها بمعدل يومي " يزيد عن 4 ساعات " بلغت 60.25%.

– **وتوضح هذه النتائج** ارتفاع مستوى حرص المبحوثين عينة الدراسة لاستخدام تطبيقات ومنصات الإعلام الجديد المتعددة عبر شبكة الانترنت، حيث أن جميع المبحوثين يستخدمونها بصفة يومية، وربما اختلاف معدلات الاستخدام بين المبحوثين يرتبط بطبيعة الاستخدام والهدف منه، فمن يستخدمونها لمتابعة الأخبار والأحداث اليومية الجارية ربما تزيد نسبتهم عن من يستخدمونها بهدف التواصل الاجتماعي مع الآخرين، أو من يستخدمونها لإجراء معاملات بيع أو شراء.

جدول (4) مقياس كثافة التعرض للتطبيقات والمنصات الرقمية عبر شبكة الانترنت

مقياس كثافة التعرض	ك	%	المتوسط الحسابي	الانحراف المعياري
منخفض	16	4.00	2.7250	0.52922
متوسط	78	19.50		
مرتفع	306	76.50		
المجموع	400	100.00		

تشير بيانات الجدول السابق إلى ما يلي:

– بناءً على الجدولين السابقين الخاصين بالتعرض للتطبيقات والمنصات الرقمية عبر شبكة الانترنت، ومعدل الاستخدام اليومي تم بناء مقياس للتعرف على كثافة هذا التعرض، وجاء التعرض (مرتفعاً) لدى 76.5% من عينة الدراسة، بينما جاءت كثافة التعرض (متوسطة) لدى 19.5%، وأخراً جاءت كثافة التعرض منخفضة لدى 4% من عينة الدراسة.

جدول رقم(5)يوضح دوافع استخدام المبحوثين لتطبيقات ومنصات الإعلام الجديد

دوافع الاستخدام	ك	%
التواصل مع الآخرين وتكوين الصداقات	311	77.75
متابعة الأخبار والأحداث الجارية	303	75.75
العمل والقيام بمهام وظيفية	264	66.00
الترفيه والألعاب وشغل الوقت	214	53.50
التحصيل العلمي والدراسة	149	37.25
ن=400		

تشير بيانات الجدول السابق إلى ما يلي:

- تباينت دوافع استخدام المبحوثين عينة الدراسة لتطبيقات ومنصات الإعلام الجديد عبر شبكة الإنترنت، وجاء في المرتبة الأولى " التواصل مع الآخرين وتكوين الصداقات "، وذلك بنسبة 77.25%، وفي المرتبة الثانية جاء " متابعة الأخبار والأحداث الجارية "، بنسبة 75.75%، ثم في المرتبة الثالثة جاء " العمل والقيام بمهام وظيفية "، بنسبة 66%، وفي المرتبة الرابعة جاء " الترفيه والألعاب وشغل الوقت " بنسبة 53.50%، وفي المرتبة الأخيرة جاء " التحصيل العلمي والدراسة "، وذلك بنسبة 37.25%.

- **وربما** هذا التباين بين المبحوثين حول دوافع استخدامهم لتطبيقات ومنصات الإعلام الجديد عبر شبكة الإنترنت يوضح مستوى الاعتماد الكبير على هذه المنصات، وبصفة خاصة منصات التواصل الاجتماعي مثل " فيس بوك ، وموقع x ، وانستغرام ، وواتس اب " وغيرها، حيث يقضى الجمهور عليها وقتاً طويلاً في التواصل مع الأخريين، أيضاً " الصحف والمواقع الإخبارية الإلكترونية، حيث متابعة الأحداث الجارية والتي تشتعل في منطقة الدول العربية، فضلاً عن توجه العديد من الدول نحو الرقمنة والتحول الرقمي في كافة القطاعات، أصبحت اغلب المعاملات تتم عبر شبكة الإنترنت، سواء كانت بدافع العمل أو بدافع التحصيل العلمي والدراسة.

جدول رقم(6) يوضح أكثر التطبيقات ومنصات الإعلام الجديد التي يستخدمها المبحوثين

تطبيقات ومنصات الإعلام الجديد	ك	%
مواقع التواصل الاجتماعي	361	90.25
تطبيقيات المعاملات المالية ومواقع البيع والشراء عبر الانترنت	321	80.25
التطبيقات المالية عبر الهواتف المحمولة	271	67.75
المواقع والصحف الإخبارية	156	39.00
البريد الإلكتروني	109	27.25
ن=400		

تشير بيانات الجدول السابق إلى ما يلي:

- أن المبحوثين عينة الدراسة يستخدمون عدة تطبيقات ومنصات للإعلام الجديد عبر شبكة الإنترنت، وجاء في مقدمتها " مواقع التواصل الاجتماعي "، وذلك بنسبة 90.25%، وفي المرتبة الثانية جاءت " تطبيقيات المعاملات المالية ومواقع البيع والشراء عبر الانترنت "، بنسبة 80.25%، تليها في المرتبة الثالثة " التطبيقات المالية عبر الهواتف المحمولة "، وذلك بنسبة 67.75%، ثم في المرتبة الخامسة جاءت " المواقع والصحف الإخبارية "، بنسبة 39%، وفي المرتبة الأخيرة جاء " البريد الإلكتروني "، وذلك بنسبة 27.25%.

- **ما أوضحته** نتائج الجدول الأسبق المتعلق بـ"دوافع استخدام المبحوثين لتطبيقات ومنصات الإعلام الجديد عبر شبكة الإنترنت"، تؤكد نتائج هذا الجدول، حيث التقت دوافع الاستخدام ومجيء " التواصل مع الآخرين وتكوين الصداقات" في مقدمتها، مع مجيء " منصات

التواصل الاجتماعي" في مقدمة المنصات التي يستخدمها المبحوثين عينة الدراسة، والتي تعد المنصات الرئيسة التي تحقق هذا الهدف.

- **كما** أن ما سبق وان أشرنا إليه في تحليل الجدول الأسبق، من أن العديد من الدول توجهت بشكل كبير نحو التحول الرقمي سواء في العمل الإداري داخل المؤسسات والهيئات أو في عمليات البيع والشراء، انعكس على اعتماد نسبة كبيرة من الجمهور على تطبيقات ومنصات الإعلام الجديدة المتعلقة بالمعاملات المالية، وهو ما أظهرته نتائج الجدول الحالي.

جدول رقم(7) يوضح مستوى حرص المبحوثين على تأمين وحماية بياناتهم الشخصية عبر تطبيقات ومنصات الإعلام الجديد التي يستخدمونها

مستوى الحرص	ك	%	المتوسط الحسابي	الانحراف المعياري
أحرص دائماً	171	42.75	2.2725	0.71380
أحرص إلى حد ما	167	41.75		
لا أحرص	62	15.50		
المجموع	400	100.00		

تشير بيانات الجدول السابق إلى ما يلي:

- ارتفاع مستوى حرص المبحوثين عينة الدراسة على تأمين وحماية بياناتهم الشخصية عبر تطبيقات ومنصات الإعلام الجديد التي يستخدمونها، بمتوسط حسابي بلغ 2.2725، حيث بلغت نسبة من يحرصون على تأمين وحماية بياناتهم الشخصية بشكل " دائم " 42.75%، بينما بلغت نسبة من يحرصون على تأمينها وحمايتها بشكل غير منتظمة " أحرص إلى حد ما "، 41.75%، في حين بلغت نسبة " من لا يحرصون على ذلك"، 15.50%.
- **وتوضح النتائج** وجود وعي لدى نسبة كبيرة من المبحوثين عينة الدراسة بأهمية تأمين وحماية بياناتهم الشخصية عبر تطبيقات ومنصات الإعلام الجديد التي يستخدمونها، ربما ارتبط ذلك بدافع منهم حول خصوصية بياناتهم وعدم رغبتهم في تعرضها لانتهاك الخصوصية من جانب الأخريين، أو حرصهم على عدم الوقوع ضحايا لسرقة هذه البيانات، وإدراكهم لخطورة ذلك وأنه من الممكن أن يعرضهم للضرر المعنوي وربما المادي.

جدول رقم(8) يوضح مستوى ثقة المبحوثين في أمان بياناتهم ومعلوماتهم عبر تطبيقات ومنصات الإعلام الجديد التي يستخدمونها

مستوى الثقة	ك	%	المتوسط الحسابي	الانحراف المعياري
أثق تماماً	153	38.25	2.3050	0.60654
أثق إلى حد ما	216	54.00		
لا أثق فيها	31	7.75		
المجموع	400	100.00		

تشير بيانات الجدول السابق إلى ما يلي:

- أن المبحوثين عينة الدراسة لا يثقون بالشكل الكافي في أمان بياناتهم ومعلوماتهم عبر تطبيقات ومنصات الإعلام الجديد التي يستخدمونها، حيث جاء في المرتبة الأولى " أثق إلى حد ما "، وذلك بنسبة 54%، بينما جاءت نسبة من يثقون " تماماً "، 38.25%، في حين بلغت نسبة من " لا يثقون في ذلك "، 7.75%.
- وربما يرجع السبب وراء عدم الثقة التامة من جانب المبحوثين عينة الدراسة في تطبيقات ومنصات الإعلام الجديد التي يستخدمونها من أن تحمي بياناتهم ومعلوماتهم، إلى ارتفاع مستوى الهجمات السيبرانية على الدول والمؤسسات وتعرضها للقرصنة الإلكترونية، خلال الفترات الماضية، وفي الوقت الراهن أيضاً، بجانب أيضاً تعرض الكثير من مستخدمي هذه التطبيقات والمنصات من الأفراد من انتهاك خصوصيتهم وتعرض بياناتهم للسرقة، واستخدامها في ابتزازهم جسدياً ومادياً.
- وتتفق نتائج الدراسة الحالية فيما توصلت إليه من عدم وجود ثقة كافية لدى مستخدمي تطبيقات ومنصات الإعلام الجديد في حمايتها لبياناتهم الشخصية من الانتهاك، مع نتائج دراسة (ريم المرموم، 2024)[41]، التي أوضحت أن الكثير من الطلاب لديهم شكوك ومخاوف من احتمالية انتهاك الخصوصية عبر منصات الإعلام الجديد، كما تتفق أيضاً في ذلك مع نتائج دراسة (Sophie C. Boerman ، 2022)[42]، التي أكدت أن المبحوثين لا يثقون في قيام منصات الإعلام الجديد بحماية بياناتهم الشخصية.

جدول رقم(9) يوضح اتجاهات المبحوثين حول مفهومهم للأمن السيبراني وانتهاكات الخصوصية

المفهوم	درجة الموافقة						المتوسط الحسابي	الانحراف المعياري	الوزن النسبي	الاتجاه
	موافق		محايد		معارض					
	ك	%	ك	%	ك	%				
نشاط إجرامي يستهدف الإضرار بالأفراد والمجتمعات	252	63.00	89	22.25	59	14.75	2.4825	0.73896	82.74	مرتفع
ابتزاز ومضايقات المستخدمين يترتب عليها خسائر مادية ومعنوية	200	50.00	140	35.00	60	15.00	2.3500	0.72720	78.33	مرتفع
اختراقات غير مشروعة لأجهزة الكمبيوتر المرتبطة بالإنترنت	186	46.50	157	39.25	57	14.25	2.3225	0.71046	77.41	متوسط
استخدام شبكة الانترنت وتطبيقاتها المختلفة بشكل سيء	160	40.00	178	44.50	62	15.50	2.2450	0.70443	74.83	متوسط
سرقة واحتيال وتصيد لمستخدمي التطبيقات والمنصات الرقمية	137	34.25	150	37.50	113	28.25	2.0600	0.78928	68.66	متوسط

تشير بيانات الجدول السابق إلى ما يلي:

- أن اتجاه المبحوثين عينة الدراسة جاء مرتفعاً نحو مفهوم الأمن السيبراني وانتهاك الخصوصية لديهم بأنه " نشاط إجرامي يستهدف الإضرار بالأفراد والمجتمعات "، بمتوسط حسابي بلغ 2.4825، حيث وافق عليه 63% من المبحوثين، بينما جاءت نسبة 22.25% منهم " محايدة "، في حين " اعترض عليه" نسبة 14.75%.
- كما جاء اتجاههم مرتفعاً نحو مفهوم " ابتزاز ومضايقات المستخدمين يترتب عليها خسائر مادية ومعنوية"، بمتوسط حسابي بلغ 2.3500، حيث وافق عليه 50% من المبحوثين، بينما جاءت نسبة 35% منهم " محايدة "، في حين " اعترض عليه" نسبة 15%.
- بينما جاء اتجاههم متوسطاً نحو مفهوم " اختراقات غير مشروعة لأجهزة الكمبيوتر المرتبطة بالإنترنت "، بمتوسط حسابي بلغ 2.3225، حيث وافق عليه 46.50% من المبحوثين، بينما جاءت نسبة 39.25% منهم " محايدة "، في حين " اعترض عليه" نسبة 14.25%.
- كما جاء اتجاههم متوسطاً نحو مفهوم " استخدام شبكة الانترنت وتطبيقاتها المختلفة بشكل سيء "، بمتوسط حسابي بلغ 2.2450، حيث وافق عليه 40% من المبحوثين، بينما جاءت نسبة 44.50% منهم " محايدة "، في حين " اعترض عليه" نسبة 15.50%.
- أيضاً جاء اتجاههم متوسطاً نحو مفهوم " سرقة واحتيال وتصيد لمستخدمي التطبيقات والمنصات الرقمية "، بمتوسط حسابي بلغ 2.0600، حيث وافق عليه 34.25% من المبحوثين، بينما جاءت نسبة 37.50% منهم " محايدة "، في حين " اعترض عليه" نسبة 28.25%.

جدول رقم(10) يوضح مصادر معرفة المبحوثين بموضوع الأمن السيبراني، وجرائم انتهاك الخصوصية

مصادر معرفة المبحوثين	ك	%
منصات التواصل الاجتماعي	297	74.25
الأصدقاء والمعارف والأقارب	196	49.00
المواقع الإلكترونية المتخصصة	177	44.25
القنوات والبرامج التليفزيونية	111	27.75
الصحف والمواقع الإخبارية	84	21.00
الكتب والمنشورات	41	10.25
ن=400		

تشير بيانات الجدول السابق إلى ما يلي:

- جاءت " منصات التواصل الاجتماعي " في مقدمة مصادر معرفة المبحوثين بموضوع الأمن السيبراني، وجرائم انتهاك الخصوصية، وذلك بنسبة 74.25%، تليها في المرتبة

الثانية " الأصدقاء والمعارف والأقارب " بنسبة 49%، ثم في المرتبة الثالثة " المواقع الإلكترونية المتخصصة" بنسبة 44.25%، وفي المرتبة الرابعة جاءت " القنوات والبرامج التليفزيونية " بنسبة 27.57%، وفي المرتبة الخامسة جاءت " الصحف والمواقع الإخبارية " بنسبة 21%، وفي المرتبة الأخيرة جاءت " الكتب والمنشورات " بنسبة 10.25%.

- وربما مجيء " منصات التواصل الاجتماعي " في المقدمة يرجع إلى كونها في الوقت الراهن هي مصدر رئيس للمعرفة ومشاركتها سواء معلومات عامة أو تجارب شخصية للمستخدمين، حيث يميلون لطرح مشاكلهم مع جرائم انتهاك الخصوصية مع الآخرين لتقديم الإفادة لهم، وتحذيرهم من الوقوع فيها، خاصة أن هذه المنصات تعد من أبرز الوسائل التي يتم فيها انتهاك الخصوصية وسرقة بيانات من المستخدمين، كما أن الناس بطبعهم يحرصون في بعض الأوقات على مشاركة تجاربهم مع " الأصدقاء والمعارف والأقارب " لطلب المشورة أو المساعدة في اتخاذ قرار.

جدول رقم(11) يوضح مدى تعرض المبحوثين لجريمة انتهاك الخصوصية لبياناتهم عبر تطبيقات ومنصات الإعلام الجديد التي يستخدمونها

الإجابة	ك	%
نعم	77	19.25
لا	323	80.75
المجموع	400	100.00

تشير بيانات الجدول السابق إلى ما يلي:

- أكد 80.75% من المبحوثين عينة الدراسة بأنهم لم يتعرضوا لجريمة انتهاك الخصوصية لبياناتهم عبر تطبيقات ومنصات الإعلام الجديد التي يستخدمونها، بينما نسبة 19,52%، أشاروا إلى أنهم تعرضوا لهذه الجرائم.

- وربما النسبة الأكبر لم تتعرض لهذه الجرائم لأن يحرصون على توقير قدر كبير من الحماية والتأمين لبياناتهم الشخصية عبر منصات الإعلام الجديد، أو يتبعون تعليمات هذه المنصات وإرشاداتها التي توفرها للمستخدمين لتعريفهم بكيفية حماية بياناتهم من السرقة، وحفظ خصوصياتهم من الانتهاك، كما أن وجود نسبة من المبحوثين تعرضت لانتهاك خصوصيتهم عبر منصات الإعلام الجديد يرتبط بعدم معرفتهم بالشكل الكافي بطرق حماية بياناتهم الشخصية، أو ربما لأنهم يمتلكون صفحات خاصة بهم تحظي بنسبة كبيرة من المتابعين، حيث تكون هذه الصفحات في الغالب هدفاً من منتهكي الخصوصية ومجرمي الانترنت، لمعرفتهم بأنها تمثل قيمة لدى مالكيها.

جدول رقم(12) يوضح مدى معرفة المبحوثين بأن نشر بياناتهم الشخصية دون إذن منهم يعد انتهاكاً لخصوصيتهم وفعلا مخالفا للقانون

الإجابة	ك	%
نعم	214	53.50
لا	186	46.50
المجموع	400	100.00

تشير بيانات الجدول السابق إلى ما يلي:

- أن نسبة 53.50% من المبحوثين عينة الدراسة يعلمون بأن نشر بياناتهم الشخصية دون إذن منهم يعد انتهاكاً لخصوصيتهم وفعلا مخالفا للقانون يعرض مرتكبيه للعقوبة، بينما نسبة 46.50% ليس لديهم معرفة بذلك.
- وتشير هذه النتائج إلى وجود نسبة كبيرة من المبحوثين ليس لديهم معرفة كاملة بوجود قوانين تجرم انتهاك خصوصيتهم عبر منصات الإعلام الجديد التي يستخدمونها، والتي تعد نشر بياناتهم الشخصية دون إذن منهم انتهاكا لخصوصيتهم، حيث يتوارد إلى أذهان الكثير من المستخدمين لمنصات الإعلام الجديد بأنهم بمجرد وضع بياناتهم الشخصية على هذه المنصات فمن الحق الآخرين مشاركتها دون إذن منهم، وهذه النتائج تفتح الباب أمام دور الحكومات ووسائل الإعلام في نشر المعرفة وتوعية الجمهور بحقوقهم في عصر البيانات المفتوحة.
- وتتفق نتائج الدراسة الحالية فيما توصلت إليه في ذلك، مع نتائج دراسة (هاني إبراهيم محمد، 2022)[43]، بأن استخدام معلوماتهم الشخصية من قبل أي شخص هو جريمة الكترونية يعاقب عليها القانون، كما تتفق أيضاً_ إلى حد ما_ مع ما توصلت إليه نتائج دراسة (Anakha Prakash، 2024)[44]، مع أنه لا يزال هناك الكثير منها الأشخاص الذين ليس لديهم معرفة بكيفية الحفاظ على أمانهم أثناء الاتصال بالإنترنت، فهناك تفاوتاً بين المبحوثين في درجة معرفتهم ووعيهم بالأمن السيبراني.

جدول رقم (13) يوضح ردود فعل المبحوثين حال تعرضهم لاختراق خصوصيتهم عبر أحد تطبيقات ومنصات الإعلام الجديد التي يستخدمونها

ردود فعل المبحوثين	ك	%
إبلاغ رجال الشرطة والجهات المعنية	211	52.75
تحذير الأهل والأصدقاء من إمكانية تعرضهم لما تعرضت له	184	46.00
سأقلل من تفاعلي على هذا التطبيق أو المنصة	147	36.75
سأوقف تعاملي واستخدامي لهذه المنصات	69	17.25
سأكتفي بتغيير كلمة المرور الخاصة بي	60	15.00
سأقوم بإغلاق حسابي وإنشاء حساب جديد عبر هذا التطبيق أو المنصة	23	5.75
ن=400		

تشير بيانات الجدول السابق إلى ما يلي:

- أظهر المبحوثون عينة الدراسة ايجابيتهم حال تعرضهم لاختراق خصوصيتهم عبر أحد تطبيقات ومنصات الإعلام الجديد التي يستخدمونها، حيث أكدوا أنهم سيتخذون ردود فعل نحوها، لكنها متباينة بينهم، فنسبة 52.75% من عينة الدراسة أفادت بأنها " ستقوم بإبلاغ رجال الشرطة والجهات المعنية "، بينما نسبة 46%، ستقوم " بتحذير الأهل والأصدقاء من إمكانية تعرضهم لما تعرضت له"، في حين أن نسبة 36.75%، أوضحت أنها " ستقلل من تفاعلها على التطبيق أو المنصة التي تم اخترقا خصوصيتها من خلالها"، كما أن نسبة 17.25% من المبحوثين أفادوا بأنه "سيوقفون تعاملهم واستخدامهم لهذه المنصات"، وأن نسبة 15% أشارت بأنها " ستكتفي بتغيير كلمة المرور الخاصة بها " وأن نسبة 5.75%، "ستقوم بإغلاق حسابها وإنشاء حساب جديد عبر هذا التطبيق أو المنصة".
- على الرغم من تباين ردود فعل الجمهور نحو تعرضهم لانتهاك خصوصيتهم عبر منصات الإعلام الجديد التي يستخدمونها إلا أنها جميعاً يمكن وصفها بأنها ايجابية، حيث تأتي على أكثر من مستوى، فبعضهم يكتفي بمستوى أكثر أمناً له ويقوم بإبلاغ الشرطة والجهات المعنية، والبعض الآخر يتخذ رد فعل أقل حدة حيث سيكتفي بتحذير الأهل والأصدقاء، وآخرين سيكتفون بغلق حساباتهم عبر المنصة كأسلوب عقابي لها بوصفها غير آمنة.

جدول رقم(14) يوضح اتجاهات نحو السلوكيات التي يتبعونها للحفاظ على بياناتهم وعدم انتهاك خصوصيتهم عبر تطبيقات ومنصات الإعلام الجديد

السلوكيات	الدرجة						المتوسط الحسابي	الانحراف المعياري	الوزن النسبي	الاتجاه
	دائماً		أحياناً		نادراً					
	ك	%	ك	%	ك	%				
تسجيل الخروج من الحسابات عقب انتهاء استخدامها مباشرة	314	78.50	75	18.75	11	2.75	2.7575	0.48917	91.91	مرتفع
إنشاء كلمات سر بشكل معقد بحيث يصعب توقعها، وتنويعها لكل حساب	313	78.25	72	18.00	15	3.75	2.7450	0.51540	91.49	مرتفع
عدم الدخول على روابط أو صفحات أو قبول صداقات من جهات مجهولة	308	77.00	65	16.25	27	6.75	2.7025	0.58724	90.07	مرتفع
لا أسجل بياناتي كاملة على حساباتي في المنصات الرقمية	301	75.25	75	18.75	24	6.00	2.6925	0.57774	89.74	مرتفع
أقوم بتعطيل الوصول إلى بيانات	302	75.50	57	14.25	41	10.25	2.6525	0.65789	88.41	مرتفع

السلوكيات	الدرجة						المتوسط الحسابي	الانحراف المعياري	الوزن النسبي	الاتجاه
	دائماً		أحياناً		نادراً					
	ك	%	ك	%	ك	%				
تسجيل الخروج من الحسابات عقب انتهاء استخدامها مباشرة	314	78.50	75	18.75	11	2.75	2.7575	0.48917	91.91	مرتفع
إنشاء كلمات سر بشكل معقد بحيث يصعب توقعها، وتنويعها لكل حساب	313	78.25	72	18.00	15	3.75	2.7450	0.51540	91.49	مرتفع
تحديد الموقع الجغرافي للتطبيقات الرقمية										
أراجع وأتحقق من الأذونات التي تتطلبها التطبيقات عند تنزيلها	291	72.75	72	18.00	37	9.25	2.6350	0.64639	87.82	مرتفع
لا أربط حساباتي الشخصية على المنصات الاجتماعية بمواقع أخرى	281	70.25	88	22.00	31	7.75	2.6250	0.62478	87.49	مرتفع
استخدام خصائص الأمان والحماية التي تتيحها المنصات الرقمية	278	69.50	93	23.25	29	7.25	2.6225	0.61721	87.41	مرتفع
أقم بتثبيت برامج موثوقة لمكافحة الفيروسات والبرامج الضارة	289	72.25	63	15.75	48	12.00	2.6025	0.69332	86.74	مرتفع
لا أقوم بتحميل التطبيقات الإلكترونية من مصادر مجهولة	228	57.00	103	25.75	69	17.25	2.3975	0.76548	79.91	مرتفع
أتجنب وضع الصور والفيديوهات الشخصية على حسابات المنصات الرقمية	190	47.50	150	37.50	60	15.00	2.3250	0.72158	77.49	متوسط

تشير بيانات الجدول السابق إلى ما يلي:

- جاء اتجاه المبحوثين عينة الدراسة نحو السلوكيات التي يتبعونها للحفاظ على بياناتهم وعدم انتهاك خصوصيتهم عبر تطبيقات ومنصات الإعلام الجديد " مرتفعاً " بصفة عامة في جميع إجاباتهم، وجاء في مقدمة هذه السلوكيات " تسجيل الخروج من الحسابات عقب انتهاء استخدامها مباشرة" بمتوسط حسابي بلغ 2.7575، وفي المرتبة الثانية جاء " إنشاء كلمات سر بشكل معقد بحيث يصعب توقعها، وتنويعها لكل حساب" بمتوسط حسابي بلغ 2.7450، وفي المرتبة الثالثة جاء سلوك " عدم الدخول على روابط أو صفحات أو قبول صداقات من جهات مجهولة" بمتوسط حسابي بلغ 2.7025، وفي المرتبة الرابعة جاء " لا أسجل بياناتي كاملة على حساباتي في المنصات الرقمية" بمتوسط حسابي بلغ 2.6925.
- وفي المرتبة الخامسة جاء سلوك " أقوم بتعطيل الوصول إلى بيانات تحديد الموقع الجغرافي للتطبيقات الرقمية" بمتوسط حسابي بلغ 2.6525، وفي المرتبة السادسة جاء " أراجع وأتحقق من الأذونات التي تتطلبها التطبيقات عند تنزيلها" بمتوسط حسابي بلغ 2.6350، وجاء في المرتبة السابعة " لا أربط حساباتي الشخصية على المنصات الاجتماعية بمواقع أخرى" بمتوسط حسابي بلغ 2.6250، وفي المرتبة الثامنة جاء " استخدام خصائص الأمان والحماية التي تتيحها المنصات الرقمية" بمتوسط حسابي بلغ 2.6225، وفي المرتبة التاسعة جاء " أقم بتثبيت برامج موثوقة لمكافحة الفيروسات والبرامج الضارة" بمتوسط حسابي بلغ 2.6025، وفي المرتبة العاشرة جاء " لا أقوم بتحميل التطبيقات الإلكترونية من مصادر مجهولة " بمتوسط حسابي بلغ 2.3975، وفي المرتبة الأخيرة بمستوى متوسط جاء " أتجنب وضع الصور والفيديوهات الشخصية على حسابات المنصات الرقمية " بمتوسط حسابي بلغ 2.3250.
- **ولعل** المستوى المرتفع لدى المبحوثين عينة الدراسة في كافة إجاباتهم حول التصرفات والسلوكيات التي يتبعونها للحفاظ على بياناتهم وعدم انتهاك خصوصيتهم عبر تطبيقات ومنصات الإعلام الجديد يشير إلى مستوى مرتفع من الوعي بأهمية ذلك، وربما ارتبط ذلك بخوفهم من تعرض بياناتهم للسرقة وما ينتج عن ذلك من أثر سلبي وضرر مادي ومعنوي محتمل، وبالتالي نمت لديهم معرفة بالأمن السيبراني وما يعنيه من مكافحة الأضرار الناجمة عن جرائم الانترنت والتي منها انتهاك الخصوصية.
- **وتتفق نتائج الدراسة** الحالية فيما توصلت إليه من ارتفاع مستوى سلوكيات المبحوثين التي يتبعونها للحفاظ على بياناتهم وعدم انتهاك خصوصيتهم عبر تطبيقات ومنصات الإعلام الجديد، مع ما توصلت إليه دراسة (هدير محمود، 2023)[45]، من أن نسبة 68% كان لديهم مستوى مرتفع من الالتزام بسلوكيات حماية الأمن السيبراني.

جدول رقم(15) الأسباب المؤدية لانتشار جرائم انتهاك الخصوصية عبر تطبيقات ومنصات الإعلام الجديد من وجهة نظر المبحوثين عينة الدراسة

الأسباب	درجة الموافقة						المتوسط الحسابي	الانحراف المعياري	الوزن النسبي	الاتجاه
	موافق		محايد		معارض					
	ك	%	ك	%	ك	%				
عدم اكتشاف هذه الوقائع إلا بعد فترة زمنية طويلة بما يصعب تجنبها	166	41.50	221	55.25	13	3.25	2.3825	0.54950	79.41	مرتفع
عدم إبلاغ الضحايا عن تعرضهم لهذه الجريمة بما يساعد على تكرارها	186	46.50	156	39.00	58	14.50	2.3200	0.71335	77.33	متوسط
ضعف القواعد التشريعية والقانونية المتخصصة في مكافحة انتهاك الخصوصية	175	43.75	175	43.75	50	12.50	2.3125	0.68265	77.08	متوسط
تزايد التطبيقات الرقمية غير المرخصة من الجهات المعنية داخل الدول	166	41.50	178	44.50	56	14.00	2.2750	0.69324	75.83	متوسط
عدم معرفة المجرمين لأنهم يعملون بشكل خفي	150	37.50	185	46.25	65	16.25	2.2125	0.70255	73.74	متوسط
الرغبة في الثراء السريع فيلجؤون لسرقة بيانات المستخدمين لابتزازهم ماليا	143	35.75	195	48.75	62	15.50	2.2025	0.68751	73.41	متوسط
عدم دراية المستخدمين للمنصات الرقمية بآليات حماية بياناتهم الشخصية	119	29.75	209	52.25	72	18.00	2.1175	0.68180	70.58	متوسط
عدم القدرة في الوصول إلى المجرمين وإخضاعهم للقانون.	122	30.50	202	50.50	76	19.00	2.1150	0.69497	70.49	متوسط

تشير بيانات الجدول السابق إلى ما يلي:

- أرجع المبحوثين عينة الدراسة انتشار جرائم انتهاك الخصوصية عبر تطبيقات ومنصات الإعلام الجديد إلى عدة أسباب، وجاء اتجاههم نحوه هذه الأسباب متوسطاً بصفة عامة، وفي مقدمة هذه الأسباب جاء " عدم اكتشاف هذه الوقائع إلا بعد فترة زمنية طويلة بما يصعب تجنبها" بمتوسط حسابي بلغ 2.3825، وفي المرتبة الثانية جاء " عدم إبلاغ الضحايا عن تعرضهم لهذه الجريمة بما يساعد على تكرارها " بمتوسط حسابي بلغ

2.3200، وفي المرتبة الثالثة جاء " ضعف القواعد التشريعية والقانونية المتخصصة في مكافحة انتهاك الخصوصية " بمتوسط حسابي بلغ 2.3125، وفي المرتبة الرابعة جاء " تزايد التطبيقات الرقمية غير المرخصة من الجهات المعنية داخل الدول " بمتوسط حسابي بلغ 2.2750.

- وفي المرتبة الخامسة جاء "عدم معرفة المجرمين لأنهم يعملون بشكل خفي " بمتوسط حسابي بلغ 2.2125، وفي المرتبة السادسة جاء " الرغبة في الثراء السريع واللجوء لسرقة بيانات المستخدمين لابتزازهم ماليا " بمتوسط حسابي بلغ 2.2025، وجاء في المرتبة السابعة " عدم دراية المستخدمين للمنصات الرقمية بآليات حماية بياناتهم الشخصية " بمتوسط حسابي بلغ 2.1175، وفي المرتبة الأخيرة بمستوى متوسط جاء " عدم القدرة في الوصول إلى المجرمين وإخضاعهم للقانون" بمتوسط حسابي بلغ 2.1150.

جدول رقم(16) يوضح اتجاه المبحوثين نحو دوافع انتهاك الخصوصية عبر تطبيقات ومنصات الإعلام الجديد

العبارات	درجة الموافقة						المتوسط الحسابي	الانحراف المعياري	الوزن النسبي	الاتجاه
	موافق		محايد		معارض					
	ك	%	ك	%	ك	%				
تحقيق مكاسب مادية باستغلال مهارات التعامل غير الأخلاقية مع الانترنت	213	53.25	162	40.50	25	6.25	2.4700	0.61240	82.33	مرتفع
الانتقام من الأشخاص والإساءة لهم والتشهير بهم	214	53.50	156	39.00	30	7.50	2.4600	0.63198	81.99	مرتفع
سرقة الهوية وانتحال الشخصية وارتكاب أفعال إجرامية بها	212	53.00	157	39.25	31	7.75	2.4525	0.63542	81.74	مرتفع
سرقة البيانات واستخدامها في مجالات التسويق والبيع	203	50.75	168	42.00	29	7.25	2.4350	0.62590	81.16	مرتفع
الوصول لتفاصيل الحسابات البنكية	194	48.50	173	43.25	33	8.25	2.4025	0.63758	80.08	مرتفع

العبارات	درجة الموافقة						المتوسط الحسابي	الانحراف المعياري	الوزن النسبي	الاتجاه
	موافق		محايد		معارض					
	ك	%	ك	%	ك	%				
تحقيق مكاسب مادية باستغلال مهارات التعامل غير الأخلاقية مع الانترنت	213	53.25	162	40.50	25	6.25	2.4700	0.61240	82.33	مرتفع
الانتقام من الأشخاص والإساءة لهم والتشهير بهم	214	53.50	156	39.00	30	7.50	2.4600	0.63198	81.99	مرتفع
للأفراد والمؤسسات وسرقتها										
التنمر والسخرية من الآخرين	163	40.75	200	50.00	37	9.25	2.3150	0.63386	77.16	متوسط
التسلية والترفيه والتلاعب بالآخرين	133	33.25	232	58.00	35	8.75	2.2450	0.60073	74.83	متوسط

تشير بيانات الجدول السابق إلى ما يلي:

- جاء اتجاه المبحوثين عينة الدراسة نحو دوافع انتهاك الخصوصية عبر تطبيقات ومنصات الإعلام الجديد " مرتفعاً " بصفة عامة، وقد جاء في مقدمة هذه الدوافع " تحقيق مكاسب مادية باستغلال مهارات التعامل غير الأخلاقية مع الانترنت " بمتوسط حسابي بلغ 2.4700، وفي المرتبة الثانية جاء " الانتقام من الأشخاص والإساءة لهم والتشهير بهم " بمتوسط حسابي بلغ 2.4600، وفي المرتبة الثالثة جاء " سرقة الهوية وانتحال الشخصية وارتكاب أفعال إجرامية بها " بمتوسط حسابي بلغ 2.4525، وفي المرتبة الرابعة جاء " سرقة البيانات واستخدامها في مجالات التسويق والبيع " بمتوسط حسابي بلغ 2.4350، وفي المرتبة الخامسة جاء " الوصول لتفاصيل الحسابات البنكية للأفراد والمؤسسات وسرقتها " بمتوسط حسابي بلغ 2.4025.
- كما جاء اتجاههم " متوسطاً " نحو دوافع انتهاك الخصوصية عبر تطبيقات ومنصات الإعلام الجديد " مرتفعاً " وذلك في دافع " التنمر والسخرية من الآخرين " بمتوسط حسابي بلغ 2.3150، وفي دافع " التسلية والترفيه والتلاعب بالآخرين " بمتوسط حسابي بلغ 2.2450.

- نتائج المبحوثين واتجاههم نحو دوافع انتهاك الخصوصية عبر تطبيقات ومنصات الإعلام الجديد، تقترب من الواقع بشكل كبير، فمنتهكي الخصوصية يرغبون في المقام الأول بجني الأموال من وراء هذه الأفعال الإجرامية بطرق غير مشروعة، سواء كان هؤلاء من خارج الدولة التي يسكنها الضحية، أو من داخلها، كما أن جزءا منها يرتبط بالانتقام من أشخاص بعينهم بالتشهير بهم أو الإساءة لهم في المجتمع، وجزء آخر في هذه الجرائم يتم ارتكابه بدافع انتحال الشخصية واستخدامها بطرق غير مشروعة في إجراء معاملات بيع وشراء، لكن دافعي " التنمر والسخرية من الآخرين، والتسلية والترفيه والتلاعب بالآخرين" أقل في المستوى من الدوافع السابقة، لأن عمليات سرقة البيانات وانتهاك الخصوصية تحتاج لوقت طويل من المجرمين ومن المستبعد بعض الشيء أن تتم فقط لمجرد التسلية أو التلاعب بالآخرين.

جدول رقم(17) يوضح اتجاه المبحوثين نحو الأضرار والآثار السلبية لمخاطر انتهاك الخصوصية على مستوى الأفراد

الآثار السلبية	درجة الموافقة						المتوسط الحسابي	الانحراف المعياري	الوزن النسبي	الاتجاه
	موافق		محايد		معارض					
	ك	%	ك	%	ك	%				
الابتزاز المادي للأفراد عبر سرقة الصور والفيديوهات	218	54.50	154	38.50	28	7.00	2.4750	0.62478	82.49	مرتفع
الاحتيال والنصب وسرقة الأموال والحسابات البنكية	190	47.50	171	42.75	39	9.75	2.3775	0.65656	79.24	مرتفع
انتحال الشخصيات وارتكاب جرائم تضر بأصحاب الشخصيات الحقيقية	168	42.00	193	48.25	39	9.75	2.3225	0.64384	77.41	متوسط
تشويه السمعة والإضرار بها	163	40.75	197	49.25	40	10.00	2.3075	0.64341	76.91	متوسط
انتحار بعض الأفراد نتيجة ضغوط والتهديدات المستمرة	150	37.50	199	49.75	51	12.75	2.2475	0.66509	74.91	متوسط
السخرية وإفساد حياة الأفراد عبر تزييف البيانات وتحريفها	135	33.75	208	52.00	57	14.25	2.1950	0.66564	73.16	متوسط
فقدان البعض لوظائفهم بسبب الأضرار النفسية لهم	129	32.25	211	52.75	60	15.00	2.1725	0.66622	72.41	متوسط
الابتزاز المعنوي والقيام بأعمال جنسية تحت التهديد	125	31.25	194	48.50	81	20.25	2.1100	0.71004	70.33	متوسط

تشير بيانات الجدول السابق إلى ما يلي:

- تباينت اتجاهات المبحوثين عينة الدراسة نحو الأضرار والآثار السلبية لمخاطر انتهاك الخصوصية على مستوى الأفراد، فقد جاء اتجاههم " مرتفعاً " نحو ضرر " الابتزاز المادي للأفراد عبر سرقة الصور والفيديوهات " حيث بلغ المتوسط الحسابي 2.4750، كما جاء اتجاههم " مرتفع " أيضا نحو ضرر " الاحتيال والنصب وسرقة الأموال والحسابات البنكية " بمتوسط حسابي بلغ 2.3775، وربما ذلك لأن الدافع الأقوى والأكثر احتمالية هو تحقيق المكاسب المادية، وان أكثر هذه الأضرار هي الأكثر تحققاً من وراء ارتكاب هذه الجرام.
- في حين جاء اتجاه المبحوثين عينة الدراسة "متوسطاً" نحو الأضرار والآثار السلبية لمخاطر انتهاك الخصوصية على مستوى الأفراد، وذلك فيما يتعلق بـ" انتحال الشخصيات وارتكاب جرائم تضر بأصحاب الشخصيات الحقيقية" حيث بلغ المتوسط الحسابي 2.3225، وأيضا في" تشويه السمعة والإضرار بها" بمتوسط حسابي بلغ 2.3075، وفي " انتحار بعض الأفراد نتيجة ضغوط والتهديدات المستمرة" بمتوسط حسابي بلغ 2.2475، وكذلك جاء متوسطا في" السخرية وإفساد حياة الأفراد عبر تزييف البيانات وتحريفها" بمتوسط حسابي بلغ 2.1950، وكذلك في" فقدان البعض لوظائفهم بسبب الأضرار النفسية لهم" بمتوسط حسابي بلغ 2.1725، وأخيرا في"الابتزاز المعنوي والقيام بأعمال جنسية تحت التهديد" بمتوسط حسابي بلغ 2.1100، وربما مجيء هذه الآثار والنتائج المترتبة على عملية انتهاك الخصوصية " متوسطة " بصفة عامة، لأن نسبة كبيرة من عينة الدراسة استبعدت حدوثها وكان اتجاههم نحوها " محايد " في النسبة الأغلب، خاصة أنها مرتبطة بمستوى الأفراد.

جدول رقم(18)يوضح اتجاه المبحوثين نحو الأضرار والآثار السلبية لمخاطر انتهاك الخصوصية على مستوى المجتمع

الآثار السلبية على المجتمع	درجة الموافقة						المتوسط الحسابي	الانحراف المعياري	الوزن النسبي	الاتجاه
	موافق		محايد		معارض					
	ك	%	ك	%	ك	%				
سرقة الحسابات البنكية للمؤسسات بما يضر بالاقتصاد القومي	297	74.25	97	24.25	6	1.50	2.7275	0.47835	90.91	مرتفع
إثارة الفوضى والفتن والاضطرابات داخل المجتمع	274	68.50	107	26.75	19	4.75	2.6375	0.57176	87.91	مرتفع
إمكانية خلق أزمات دبلوماسية بين الدول	263	65.75	118	29.50	19	4.75	2.6100	0.57770	86.99	مرتفع
تشويه رموز المجتمع بما يشكك في مصداقيتهم بعدها	243	60.75	133	33.25	24	6.00	2.5475	0.60718	84.91	مرتفع
الضحايا قد يلجؤون إلى الانتقام بما يساعد على انتشار الجريمة في المجتمع	223	55.75	128	32.00	49	12.25	2.4350	0.70143	81.16	مرتفع
قد تؤدي إلى التشكيك في العمل المجتمعي من جانب الحكومات مثل تزييف نتائج الانتخابات	180	45.00	191	47.75	29	7.25	2.3775	0.61721	79.24	مرتفع
تهديد الأمن القومي للدولة بسرقة بيانات مؤسساتها ومواطنيها	159	39.75	212	53.00	29	7.25	2.3250	0.60439	77.49	متوسط
انتشار الإرهاب الالكتروني في المجتمع والخوف من التكنولوجيا الحديثة	111	27.75	245	61.25	44	11.00	2.1675	0.60029	72.24	متوسط
تساعد على هدم قيم المجتمع وأخلاقياته	128	32.00	160	40.00	112	28.00	2.0400	0.77453	67.99	متوسط

تشير بيانات الجدول السابق إلى ما يلي:

- جاء اتجاه المبحوثين عينة الدراسة نحو الأضرار والآثار السلبية المحتملة لمخاطر انتهاك الخصوصية على مستوى المجتمع" مرتفعاً "، في العديد من هذه الأضرار، وفي مقدمتها " سرقة الحسابات البنكية للمؤسسات بما يضر بالاقتصاد القومي " حيث بلغ المتوسط الحسابي 2.7275، وفي" إثارة الفوضى والفتن والاضطرابات داخل المجتمع " بمتوسط حسابي بلغ 2.6375، وفي" إمكانية خلق أزمات دبلوماسية بين الدول " بمتوسط حسابي بلغ 2.6100، وفي" تشويه رموز المجتمع بما يشكك في مصداقيتهم بعدها "بمتوسط حسابي بلغ 2.5475، وفي" الضحايا قد يلجؤون إلى الانتقام بما يساعد على انتشار الجريمة في المجتمع " بمتوسط حسابي بلغ 2.4350، وفي " قد تؤدي إلى التشكيك في العمل المجتمعي من جانب الحكومات مثل تزييف نتائج الانتخابات" بمتوسط حسابي بلغ 2.3775.
- في حين جاء اتجاههم " متوسطاً " بصفة عامة نحو " تهديد الأمن القومي للدولة بسرقة بيانات مؤسساتها ومواطنيها" حيث بلغ المتوسط الحسابي 2.3250، وفي " انتشار الإرهاب الالكتروني في المجتمع والخوف من التكنولوجيا الحديثة" بمتوسط حسابي بلغ 2.1675، وفي " تساعد على هدم قيم المجتمع وأخلاقياته" بمتوسط حسابي بلغ 2.0400.

جدول رقم(19) يوضح مقترحات المبحوثين للحد من ظاهرة انتهاك الخصوصية ومكافحتها عبر تطبيقات ومنصات الإعلام الجديد

مقترحات المبحوثين	ك	%
التوعية الأسرية للأبناء وخاصة صغار السن بكيفية التعامل الآمن مع الانترنت	331	82.75
العمل على محو الأمية التكنولوجية في المجتمعات	309	77.25
تكثيف حملات التوعية باليات الحماية من انتهاك الخصوصية والتعامل معها	297	74.25
التوسع في سن القوانين والتشريعات التي تجرمها وتفعيل تطبيقها	288	72.00
تشجيع الضحايا على الإبلاغ عن جرائم انتهاك الخصوصية التي يتعرضون لها	274	68.50
تقوية البنية التكنولوجية للدول وتعزيز أمنها السيبراني	265	66.25
ن=400		

تشير بيانات الجدول السابق إلى ما يلي:

- قدم المبحوثين عينة الدراسة عدداً من المقترحات للحد من ظاهرة انتهاك الخصوصية ومكافحتها عبر تطبيقات ومنصات الإعلام الجديد، جاء في مقدمتها " التوعية الأسرية للأبناء وخاصة صغار السن بكيفية التعامل الآمن مع الانترنت" وذلك بنسبة بلغت 82.75%، يليه في المرتبة الثانية " العمل على محو الأمية التكنولوجية في المجتمعات" بنسبة بلغت 77.25%، ثم في المرتبة الثالثة " تكثيف حملات التوعية باليات الحماية من انتهاك الخصوصية والتعامل معها" بنسبة بلغت 74.25%، وفي المرتبة الرابعة جاء " التوسع في سن القوانين والتشريعات التي تجرمها وتفعيل تطبيقها" بنسبة بلغت 72.00%، ثم في المرتبة الخامسة " تشجيع الضحايا على الإبلاغ عن جرائم انتهاك الخصوصية التي

يتعرضون لها" بنسبة بلغت68.50 %، وفي المرتبة الأخيرة جاء مقترح " تقوية البنية التكنولوجية للدول وتعزيز أمنها السيبراني " وذلك بنسبة بلغت 66.25%.

- تشير مقترحات المبحوثين إلى ضرورة تضافر كافة الجهود للحد من هذه الظاهرة، لما لها من آثار سلبية كبيرة على الأفراد والمجتمعات، وبدأت مقترحات المبحوثين من الأسرة بصفتها المراقب الأول، حيث طالب المبحوثين بتوعية الأبناء خاصة صغار السن الذين يستخدمون منصات الإعلام الاجتماعي من خطورة انتهاك الخصوصية، وتعريفهم بطرق حماية بياناتهم، أو الإشراف عليهم بصفة شخصية من الوالدين، كما شملت مقترحات المبحوثين الدور المجتمعي الذي يقع على عاتق حكومات الدول من تكثيف مبادرات محو الأمية الرقمية للمواطنين، ومبادرات التوعية بمخاطر انتهاك الخصوصية، وسن القوانين بما يشمل تغليظ العقوبات، وصولاً إلى العمل على تقوية البنية التكنولوجية للدول وتعزيز أمنها السيبراني.
- وتتفق نتائج الدراسة الحالية فيما يتعلق باقتراحات المبحوثين، مع نتائج دراسة (Mrittika Rani، 2024)[46]، التي أكدت على ضرورة توعية عامة الناس من الطلاب وغيرهم حول الأمن السيبراني والاستخدام الأخلاقي للإنترنت، كما تتفق أيضا مع نتائج دراسة (نهي مجدي محمد، 2021)[47]، التي أكدت ضرورة وجود قواعد تشريعية وقانونية رادعة لدعـم تحقيـق الأمن السـيبراني.

نتائج اختبار فروض الدراسة:

الفرض الأول: توجد علاقة ارتباطية ذات دلالة إحصائية بين مستوى حرص المبحوثين عينة الدراسة على تأمين وحماية بياناتهم الشخصية من الانتهاك، وبين اتجاههم نحو سلوكياتهم في الحفاظ عليها.

جدول (20) معامل ارتباط بيرسون لقياس العلاقة بين مستوى حرص المبحوثين عينة الدراسة على تأمين وحماية بياناتهم الشخصية من الانتهاك، وبين اتجاههم نحو سلوكياتهم في الحفاظ عليها

المتغيرات	مستوى حرص المبحوثين عينة الدراسة على تأمين وحماية بياناتهم الشخصية من الانتهاك			
	معامل الارتباط بيرسون	مستوى الدلالة	نوع العلاقة	العدد
سلوكيات المبحوثين لتأمين وحماية بياناتهم الشخصية من الانتهاك	0.571**	0.000	طردية متوسطة القوة	400

تشير بيانات الجدول السابق إلى الآتي:

- وجود علاقة دالة احصائياً بين مستوى حرص المبحوثين عينة الدراسة على تأمين وحماية بياناتهم الشخصية من الانتهاك، وبين سلوكياتهم في الحفاظ عليها، حيث بلغ معامل الارتباط بيرسون (0.571) وهي دالة عند مستوى معنوية (0.000)، وهي علاقة طردية

متوسطة القوة، أي كلما زاد مستوى حرص المبحوثين عينة الدراسة على تأمين وحماية بياناتهم الشخصية من الانتهاك، كلما زادت سلوكياتهم نحو تأمين وحماية بياناتهم الشخصية من الانتهاك، والعكس بالعكس.

- وبذلك يقبل الفرض العلمي القائل بوجود علاقة ارتباطية ذات دلالة إحصائية بين مستوى حرص المبحوثين عينة الدراسة على تأمين وحماية بياناتهم الشخصية من الانتهاك، وبين اتجاههم نحو سلوكياتهم في الحفاظ عليها.

الفرض الثاني: توجد علاقة ارتباطية ذات دلالة إحصائية بين سلوكيات المبحوثين لتأمين ولحماية بياناتهم الشخصية من الانتهاك والأضرار، واتجاههم نحو الآثار السلبية لمخاطر انتهاك الخصوصية على مستوى الفرد والمجتمع.

جدول (21) معامل ارتباط بيرسون لقياس العلاقة بين اتجاه المبحوثين نحو سلوكيات تأمين وحماية بياناتهم الشخصية من الانتهاك والأضرار، واتجاههم نحو الآثار السلبية لمخاطر انتهاك الخصوصية على مستوى الفرد والمجتمع

المتغيرات	سلوكيات المبحوثين لتأمين وحماية بياناتهم الشخصية من الانتهاك والأضرار			
	معامل الارتباط بيرسون	مستوى الدلالة	نوع العلاقة	العدد
اتجاه المبحوثين نحو الآثار السلبية لمخاطر انتهاك الخصوصية على مستوى الفرد	0.363**	0.000	طردية متوسطة القوة	400
اتجاه المبحوثين نحو الآثار السلبية لمخاطر انتهاك الخصوصية على مستوى المجتمع	0.308**	0.000	طردية متوسطة القوة	400

تشير بيانات الجدول السابق إلى الآتي:

- وجود علاقة دالة احصائياً بين سلوكيات المبحوثين لتأمين ولحماية بياناتهم الشخصية من الانتهاك والأضرار، واتجاههم نحو الآثار السلبية لمخاطر انتهاك الخصوصية على مستوى الفرد، حيث بلغ معامل الارتباط بيرسون (0.363) وهي دالة عند مستوى معنوية (0.000)، وهي علاقة طردية متوسطة القوة، أي كلما زادت سلوكيات المبحوثين لتأمين ولحماية بياناتهم الشخصية من الانتهاك والأضرار، كلما زاد اتجاههم الإيجابي نحو الآثار السلبية لمخاطر انتهاك الخصوصية على مستوى الفرد، والعكس بالعكس.
- وجود علاقة دالة احصائياً بين سلوكيات المبحوثين لتأمين ولحماية بياناتهم الشخصية من الانتهاك والأضرار، واتجاههم نحو الآثار السلبية لمخاطر انتهاك الخصوصية على مستوى المجتمع، حيث بلغ معامل الارتباط بيرسون (0.308) وهي دالة عند مستوى معنوية (0.000)، وهي علاقة طردية متوسطة القوة، أي كلما زادت سلوكيات المبحوثين لتأمين

ولحماية بياناتهم الشخصية من الانتهاك والأضرار، كلما زاد اتجاههم الإيجابي نحو الآثار السلبية لمخاطر انتهاك الخصوصية على مستوى المجتمع، والعكس بالعكس.

- وبذلك يُقبل الفرض العلمي القائل بوجود علاقة ارتباطية ذات دلالة إحصائية بين سلوكيات المبحوثين لتأمين ولحماية بياناتهم الشخصية من الانتهاك والأضرار، واتجاههم نحو الآثار السلبية لمخاطر انتهاك الخصوصية على مستوى الفرد والمجتمع.

الفرض الثالث: توجد علاقة ارتباطية ذات دلالة إحصائية بين ثقة المبحوثين عينة الدراسة في حماية بياناتهم الشخصية عبر تطبيقات الإعلام الجديد التي يستخدمونها. وبين سلوكياتهم في الحفاظ عليها.

جدول (22) معامل ارتباط بيرسون لقياس العلاقة بين ثقة المبحوثين عينة الدراسة في حماية بياناتهم الشخصية عبر تطبيقات الإعلام الجديد التي يستخدمونها. وبين سلوكياتهم في الحفاظ عليها

المتغيرات	ثقة المبحوثين عينة الدراسة في حماية بياناتهم الشخصية عبر تطبيقات الإعلام الجديد التي يستخدمونها			
	معامل الارتباط بيرسون	مستوى الدلالة	نوع العلاقة	العدد
سلوكيات المبحوثين لتأمين وحماية بياناتهم الشخصية من الانتهاك	0.613**	0.000	طردية قوية	400

تشير بيانات الجدول السابق إلى الآتي:

- وجود علاقة دالة احصائياً بين ثقة المبحوثين عينة الدراسة في حماية بياناتهم الشخصية عبر تطبيقات الإعلام الجديد التي يستخدمونها، وبين سلوكياتهم في الحفاظ عليها، حيث بلغ معامل الارتباط بيرسون (0.613) وهي دالة عند مستوى معنوية (0.000)، وهي علاقة طردية قوية، أي كلما زادت ثقة المبحوثين عينة الدراسة في حماية بياناتهم الشخصية عبر تطبيقات الإعلام الجديد التي يستخدمونها، كلما زادت سلوكياتهم نحو تأمين وحماية بياناتهم الشخصية من الانتهاك، والعكس بالعكس.
- وبذلك يُقبل الفرض العلمي القائل بوجود علاقة ارتباطية ذات دلالة إحصائية بين ثقة المبحوثين عينة الدراسة في حماية بياناتهم الشخصية عبر تطبيقات الإعلام الجديد التي يستخدمونها. وبين سلوكياتهم في الحفاظ عليها.

الفرض الرابع: توجد علاقة ذات دلالة إحصائية بين كثافة استخدام المبحوثين عينة الدراسة لمنصات وتطبيقات الإعلام الجديد، وبين مستوى حرصهم على حماية بياناتهم من الاختراق.

جدول (23) معامل ارتباط بيرسون لقياس العلاقة بين كثافة استخدام المبحوثين عينة الدراسة لمنصات وتطبيقات الإعلام الجديد

المتغيرات	كثافة استخدام المبحوثين عينة الدراسة لمنصات وتطبيقات الإعلام الجديد			
	معامل الارتباط بيرسون	مستوى الدلالة	نوع العلاقة	العدد
مستوى حرص المبحوثين على حماية بياناتهم من الاختراق	0.278**	0.000	طردية ضعيفة	400

تشير بيانات الجدول السابق إلى الآتي:

- وجود علاقة دالة احصائياً بين كثافة استخدام المبحوثين عينة الدراسة لمنصات وتطبيقات الإعلام الجديد، وبين مستوى حرصهم على حماية بياناتهم من الاختراق، حيث بلغ معامل الارتباط بيرسون (0.278) وهي دالة عند مستوى معنوية (0.000)، وهي علاقة طردية ضعيفة، أي كلما زادت كثافة استخدام المبحوثين عينة الدراسة لمنصات وتطبيقات الإعلام الجديد، كلما زاد مستوى حرصهم على حماية بياناتهم من الاختراق، والعكس بالعكس.
- وبذلك يقبل الفرض العلمي القائل بوجود علاقة ارتباطية ذات دلالة إحصائية بين كثافة استخدام المبحوثين عينة الدراسة لمنصات وتطبيقات الإعلام الجديد، وبين مستوى حرصهم على حماية بياناتهم من الاختراق.

الفرض الخامس: توجد فروق ذات دلالة إحصائية بين المبحوثين عينة الدراسة في اتجاههم نحو مفهوم الأمن السيبراني وانتهاكات الخصوصية، وبين متغيراتهم الديموغرافية (النوع - السن- المستوى التعليمي- الحالة الاجتماعية - المستوى الاقتصادي).

جدول (24) نتائج اختبار (T.Test) لقياس دلالة الفروق بين المبحوثين محل الدراسة على مقياس اتجاههم نحو مفهوم الأمن السيبراني وانتهاكات الخصوصية وفقاً لمتغير النوع

المتغيرات	النوع	العدد	المتوسط الحسابي	الانحراف المعياري	قيمة T	درجات الحرية df	مستوى المعنوية Sig
اتجاه المبحوثين نحو مفهوم الأمن السيبراني وانتهاكات الخصوصية	ذكر	273	2.2374	0.41079	4.106	398	0.000
	أنثى	127	2.4094	0.34167			
	المجموع	400					

تشير بيانات الجدول السابق إلى ما يلي:

- **وجود فروق ذات دلالة إحصائية** بين المبحوثين في اتجاههم نحو مفهوم الأمن السيبراني وانتهاكات الخصوصية وفقاً لمتغير النوع، حيث بلغت قيمة "ت" (4.106)، وهي دالة عند مستوى معنوية (0.000)، أي أنه توجد اختلافات بين الذكور والإناث في اتجاههم نحو مفهوم الأمن السيبراني وانتهاكات الخصوصية، وذلك لصالح أفراد العينة من (الإناث) بمتوسط حسابي (2.4094).

جدول (25) نتائج اختبار تحليل التباين الأحادي (ANOVA) لقياس دلالة الفروق بين المبحوثين محل الدراسة على مقياس اتجاههم نحو مفهوم الأمن السيبراني وانتهاكات الخصوصية وفقاً لمتغير (السن- المستوى التعليمي- الحالة الاجتماعية - المستوى الاقتصادي).

المتغيرات	المستوى التعليمي	العدد	المتوسط الحسابي	الانحراف المعياري	قيمة F	درجات الحرية df	مستوى المعنوية Sig
اتجاه المبحوثين نحو مفهوم الأمن السيبرانى وانتهاكات الخصوصية	متوسط	99	2.3030	0.38265	0.804	2 397	0.448
	جامعي	252	2.3008	0.39860			
	دراسات عليا (ماجستير- دكتوراه)	49	2.2245	0.42550			
	المجموع	400	2.2920	0.39791			
	العمر						
	من 18 إلى أقل من 20 عام	105	2.2171	0.39722	5.235	2 397	0.006
	من 20 إلى أقل من 25 عام	109	2.2495	0.39736			
	من 25 إلى أقل من 35عام	186	2.3591	0.38966			
	المجموع	400	2.2920	0.39791			
	الحالة الاجتماعية						
	أعزب	147	2.3116	0.38898	0.289	3 396	0.833
	متزوج	238	2.2840	0.40000			
	مطلق	12	2.2333	0.47354			
	أرمل	3	2.2000	0.52915			
	المجموع	400	2.2920	0.39791			
	المستوى الاقتصادي						
	منخفض	63	2.2730	0.42850	0.154	2 397	0.857
	متوسط	223	2.3013	0.39450			
	مرتفع	114	2.2842	0.39005			
	المجموع	400	2.2920	0.39791			

تشير بيانات الجدول السابق إلى ما يلي:

- أظهر استخدام اختبار "ف" عدم وجود فروق ذات دلالة إحصائية بين المبحوثين في اتجاههم نحو مفهوم الأمن السيبراني وانتهاكات الخصوصية وفقاً لمتغير المستوى التعليمي، حيث كانت قيمة "ف" (0.804)، وهي غير دالة عند مستوى معنوية (0.448)، أي أنه ليس هناك اختلاف بين عينة الدراسة على اختلاف مستويات تعليمهم في اتجاههم نحو مفهوم الأمن السيبراني وانتهاكات الخصوصية.
- أظهر استخدام اختبار "ف" وجود فروق ذات دلالة إحصائية بين المبحوثين في اتجاههم نحو مفهوم الأمن السيبراني وانتهاكات الخصوصية وفقاً لمتغير العمر، حيث كانت قيمة "ف" (5.235)، وهي دالة عند مستوى معنوية (0.006)، أي أن هناك اختلاف بين عينة الدراسة على اختلاف أعمارهم في اتجاههم نحو مفهوم الأمن السيبراني وانتهاكات الخصوصية، وأظهر اختبار L. S.D أن ذلك الاختلاف لصالح أفراد العينة أصحاب الفئة العمرية (من 25 إلى أقل من 35عام) بمتوسط حسابي (2.3591).
- أظهر استخدام اختبار "ف" عدم وجود فروق ذات دلالة إحصائية بين المبحوثين في اتجاههم نحو مفهوم الأمن السيبراني وانتهاكات الخصوصية وفقاً لمتغير الحالة الاجتماعية، حيث كانت قيمة "ف" (0.289)، وهي غير دالة عند مستوى معنوية (0.833)، أي أنه ليس هناك اختلاف بين عينة الدراسة على اختلاف حالاتهم الاجتماعية في اتجاههم نحو مفهوم الأمن السيبراني وانتهاكات الخصوصية.
- أظهر استخدام اختبار "ف" عدم وجود فروق ذات دلالة إحصائية بين المبحوثين في اتجاههم نحو مفهوم الأمن السيبراني وانتهاكات الخصوصية وفقاً لمتغير المستوى الاقتصادي، حيث كانت قيمة "ف" (0.154)، وهي غير دالة عند مستوى معنوية (0.857)، أي أنه ليس هناك اختلاف بين عينة الدراسة على اختلاف مستويتهم الاقتصادية في اتجاههم نحو مفهوم الأمن السيبراني وانتهاكات الخصوصية.

الفرض السادس: توجد فروق ذات دلالة إحصائية بين المبحوثين عينة الدراسة في اتجاههم نحو الأضرار والآثار السلبية لمخاطر انتهاك الخصوصية على مستوى الفرد والمجتمع، وفقاً لمتغيراتهم الديموغرافية (النوع- السن- المستوى التعليمي- الحالة الاجتماعية- المستوى الاقتصادي)

جدول (26) نتائج اختبار (T.Test) لقياس دلالة الفروق بين المبحوثين محل الدراسة على مقياس اتجاههم نحو الأضرار والآثار السلبية لمخاطر انتهاك الخصوصية على مستوى الفرد والمجتمع وفقاً لمتغير النوع

المتغيرات	النوع	العدد	المتوسط الحسابي	الانحراف المعياري	قيمة T	درجات الحرية df	مستوى المعنوية Sig
الآثار على مستوى الفرد	ذكر	273	2.2463	0.52169	1.689	398	0.092
	أنثى	127	2.3396	0.49699			
الآثار على مستوى المجتمع	ذكر	273	2.4127	0.35173	1.457	398	0.146
	أنثى	127	2.4663	0.32229			

تشير بيانات الجدول السابق إلى ما يلي:

- عدم وجود فروق ذات دلالة إحصائية بين المبحوثين في اتجاههم نحو الأضرار والآثار السلبية لمخاطر انتهاك الخصوصية على مستوى الفرد وفقاً لمتغير النوع، حيث بلغت قيمة "ت" (1.689)، وهي غير دالة عند مستوى معنوية (0.092)، أي أنه لا توجد اختلافات بين الذكور والإناث في اتجاههم نحو الأضرار والآثار السلبية لمخاطر انتهاك الخصوصية على مستوى الفرد.
- عدم وجود فروق ذات دلالة إحصائية بين المبحوثين في اتجاههم نحو الأضرار والآثار السلبية لمخاطر انتهاك الخصوصية على مستوى المجتمع وفقاً لمتغير النوع، حيث بلغت قيمة "ت" (1.457)، وهي غير دالة عند مستوى معنوية (0.146)، أي أنه لا توجد اختلافات بين الذكور والإناث في اتجاههم نحو الأضرار والآثار السلبية لمخاطر انتهاك الخصوصية على مستوى المجتمع.

جدول (27) نتائج اختبار تحليل التباين الأحادي (ANOVA) لقياس دلالة الفروق بين المبحوثين محل الدراسة على مقياس اتجاههم نحو الأضرار والآثار السلبية لمخاطر انتهاك الخصوصية على مستوى الفرد والمجتمع وفقاً لمتغير المستوى التعليمي

المتغيرات	المستوى التعليمي	العدد	المتوسط الحسابي	الانحراف المعياري	قيمة F	درجات الحرية df	مستوى المعنوية Sig
الأضرار والآثار السلبية لمخاطر انتهاك الخصوصية على مستوى الفرد	متوسط	99	2.3068	0.49592	0.272	2 397	0.762
	جامعي	252	2.2693	0.51163			
	دراسات عليا (ماجستير- دكتوراه)	49	2.2474	0.57650			
	المجموع	400	2.2759	0.51519			
الأضرار والآثار السلبية لمخاطر انتهاك الخصوصية على مستوى المجتمع	متوسط	99	2.4837	0.31279	1.994	2 397	0.137
	جامعي	252	2.4193	0.35039			
	دراسات عليا (ماجستير- دكتوراه)	49	2.3741	0.35695			
	المجموع	400	2.4297	0.34317			

تشير بيانات الجدول السابق إلى ما يلي:

- أظهر استخدام اختبار "ف" عدم وجود فروق ذات دلالة إحصائية بين المبحوثين في اتجاههم نحو الأضرار والآثار السلبية لمخاطر انتهاك الخصوصية على مستوى الفرد وفقاً لمتغير المستوى التعليمي، حيث كانت قيمة "ف" (0.272)، وهي غير دالة عند مستوى معنوية (0.762)، أي أنه ليس هناك اختلاف بين عينة الدراسة على اختلاف مستويات تعليمهم في اتجاههم نحو الأضرار والآثار السلبية لمخاطر انتهاك الخصوصية على مستوى الفرد.
- أظهر استخدام اختبار "ف" عدم وجود فروق ذات دلالة إحصائية بين المبحوثين في اتجاههم نحو الأضرار والآثار السلبية لمخاطر انتهاك الخصوصية على مستوى المجتمع وفقاً لمتغير المستوى التعليمي، حيث كانت قيمة "ف" (1.994)، وهي غير دالة عند مستوى معنوية (0.137)، أي أنه ليس هناك اختلاف بين عينة الدراسة على اختلاف

مستويات تعليمهم في اتجاههم نحو الأضرار والآثار السلبية لمخاطر انتهاك الخصوصية على مستوى المجتمع.

جدول (28) نتائج اختبار تحليل التباين الأحادي (ANOVA) لقياس دلالة الفروق بين المبحوثين محل الدراسة على مقياس اتجاههم نحو الأضرار والآثار السلبية لمخاطر انتهاك الخصوصية على مستوى الفرد والمجتمع وفقاً لمتغير العمر

المتغيرات	العمر	العدد	المتوسط الحسابي	الانحراف المعياري	قيمة F	درجات الحرية df	مستوى المعنوية Sig
الأضرار والآثار السلبية لمخاطر انتهاك الخصوصية على مستوى الفرد	من 18 إلى أقل من 20 عام	105	2.3024	0.49114	1.864	2 397	0.156
	من 20 إلى أقل من 25 عام	109	2.1950	0.54044			
	من 25 إلى أقل من 35عام	186	2.3085	0.51089			
	المجموع	400	2.2759	0.51519			
الأضرار والآثار السلبية لمخاطر انتهاك الخصوصية على مستوى المجتمع	من 18 إلى أقل من 20 عام	105	2.4582	0.32273	3.827	2 397	0.023
	من 20 إلى أقل من 25 عام	109	2.3527	0.36063			
	من 25 إلى أقل من 35عام	186	2.4588	0.33869			
	المجموع	400	2.4297	0.34317			

تشير بيانات الجدول السابق إلى ما يلي:

- أظهر استخدام اختبار "ف" عدم وجود فروق ذات دلالة إحصائية بين المبحوثين في اتجاههم نحو الأضرار والآثار السلبية لمخاطر انتهاك الخصوصية على مستوى الفرد وفقاً لمتغير العمر، حيث كانت قيمة "ف" (1.864)، وهي غير دالة عند مستوى معنوية (0.156)، أي أنه ليس هناك اختلاف بين عينة الدراسة على اختلاف أعمارهم في اتجاههم نحو الأضرار والآثار السلبية لمخاطر انتهاك الخصوصية على مستوى الفرد.
- أظهر استخدام اختبار "ف" وجود فروق ذات دلالة إحصائية بين المبحوثين في اتجاههم نحو الأضرار والآثار السلبية لمخاطر انتهاك الخصوصية على مستوى المجتمع وفقاً لمتغير العمر، حيث كانت قيمة "ف" (3.827)، وهي دالة عند مستوى معنوية (0.023)، أي أن هناك اختلاف بين عينة الدراسة على اختلاف أعمارهم في اتجاههم نحو الأضرار والآثار السلبية لمخاطر انتهاك الخصوصية على مستوى المجتمع، وأظهر اختبار L. S.D أن ذلك الاختلاف لصالح أفراد العينة أصحاب الفئة العمرية (من 25 إلى أقل من 35عام) بمتوسط حسابي (2.4588).

جدول (29) نتائج اختبار تحليل التباين الأحادي (ANOVA) لقياس دلالة الفروق بين المبحوثين محل الدراسة على مقياس اتجاههم نحو الأضرار والآثار السلبية لمخاطر انتهاك الخصوصية على مستوى الفرد والمجتمع وفقاً لمتغير الحالة الاجتماعية

المتغيرات	الحالة الاجتماعية	العدد	المتوسط الحسابي	الانحراف المعياري	قيمة F	درجات الحرية df	مستوى المعنوية Sig
الأضرار والآثار السلبية لمخاطر انتهاك الخصوصية على مستوى الفرد	أعزب	147	2.2611	0.50169	0.088	3 396	0.967
	متزوج	238	2.2826	0.52970			
	مطلق	12	2.3229	0.45370			
	أرمل	3	2.2917	0.40182			
	المجموع	400	2.2759	0.51519			
الأضرار والآثار السلبية لمخاطر انتهاك الخصوصية على مستوى المجتمع	أعزب	147	2.4906	0.27551	3.076	3 396	0.028
	متزوج	238	2.3996	0.37692			
	مطلق	12	2.3519	0.32075			
	أرمل	3	2.1481	0.12830			
	المجموع	400	2.4297	0.34317			

تشير بيانات الجدول السابق إلى ما يلي:

- أظهر استخدام اختبار "ف" عدم وجود فروق ذات دلالة إحصائية بين المبحوثين في اتجاههم نحو الأضرار والآثار السلبية لمخاطر انتهاك الخصوصية على مستوى الفرد وفقاً لمتغير الحالة الاجتماعية، حيث كانت قيمة "ف" (0.088)، وهي غير دالة عند مستوى معنوية (0.967)، أي أنه ليس هناك اختلاف بين عينة الدراسة على اختلاف حالاتهم

الاجتماعية في اتجاههم نحو الأضرار والآثار السلبية لمخاطر انتهاك الخصوصية على مستوى الفرد.

- أظهر استخدام اختبار "ف" وجود فروق ذات دلالة إحصائية بين المبحوثين في اتجاههم نحو الأضرار والآثار السلبية لمخاطر انتهاك الخصوصية على مستوى المجتمع وفقاً لمتغير العمر، حيث كانت قيمة "ف" (3.076)، وهي دالة عند مستوى معنوية (0.028)، أي أن هناك اختلاف بين عينة الدراسة على اختلاف حالاتهم الاجتماعية في اتجاههم نحو الأضرار والآثار السلبية لمخاطر انتهاك الخصوصية على مستوى المجتمع، وأظهر اختبار L. S.D أن ذلك الاختلاف لصالح أفراد العينة من (العزاب) بمتوسط حسابي (2.4906).

جدول (30) نتائج اختبار تحليل التباين الأحادي (ANOVA) لقياس دلالة الفروق بين المبحوثين محل الدراسة على مقياس اتجاههم نحو الأضرار والآثار السلبية لمخاطر انتهاك الخصوصية على مستوى الفرد والمجتمع وفقاً لمتغير المستوى الاقتصادي

المتغيرات	المستوى الاقتصادي	العدد	المتوسط الحسابي	الانحراف المعياري	قيمة F	درجات الحرية df	مستوى المعنوية Sig
الأضرار والآثار السلبية لمخاطر انتهاك الخصوصية على مستوى الفرد	منخفض	63	2.1925	0.48194	1.639	2 397	0.195
	متوسط	223	2.3145	0.49545			
	مرتفع	114	2.2467	0.56552			
	المجموع	400	2.2759	0.51519			
الأضرار والآثار السلبية لمخاطر انتهاك الخصوصية على مستوى المجتمع	منخفض	63	2.4374	0.31228	0.704	2 397	0.495
	متوسط	223	2.4439	0.34117			
	مرتفع	114	2.3977	0.36356			
	المجموع	400	2.4297	0.34317			

تشير بيانات الجدول السابق إلى ما يلي:

- أظهر استخدام اختبار "ف" عدم وجود فروق ذات دلالة إحصائية بين المبحوثين في اتجاههم نحو الأضرار والآثار السلبية لمخاطر انتهاك الخصوصية على مستوى الفرد وفقاً لمتغير المستوى الاقتصادي، حيث كانت قيمة "ف" (1.639)، وهي غير دالة عند مستوى معنوية (0.195)، أي أنه ليس هناك اختلاف بين عينة الدراسة على اختلاف مستويات تعليمهم في اتجاههم نحو الأضرار والآثار السلبية لمخاطر انتهاك الخصوصية على مستوى الفرد.
- أظهر استخدام اختبار "ف" عدم وجود فروق ذات دلالة إحصائية بين المبحوثين في اتجاههم نحو الأضرار والآثار السلبية لمخاطر انتهاك الخصوصية على مستوى المجتمع وفقاً لمتغير المستوى الاقتصادي، حيث كانت قيمة "ف" (0.704)، وهي غير دالة عند مستوى معنوية (0.495)، أي أنه ليس هناك اختلاف بين عينة الدراسة على اختلاف

مستويات تعليمهم في اتجاههم نحو الأضرار والآثار السلبية لمخاطر انتهاك الخصوصية على مستوى المجتمع.

خاتمة الدراسة:

- أن مستوى استخدام المبحوثين عينة الدراسة للتطبيقات ومنصات الإعلام الجديد المختلفة عبر شبكة الانترنت جاء مرتفعا، بمتوسط حسابي بلغ 2.6875، وتشير هذه البيانات إلى أن نسبة كبيرة من المبحوثين تعتمد بشكل يومي على منصات التواصل الاجتماعي مثل فيسبوك، تويتر، وإنستغرام للحصول على الأخبار والمعلومات، مما يعكس تحولاً نحو وسائل الإعلام الجديدة كمصادر رئيسية للمعلومات.
- تباينت دوافع استخدام المبحوثين عينة الدراسة لتطبيقات ومنصات الإعلام الجديد عبر شبكة الإنترنت، وجاء في المرتبة الأولى " التواصل مع الآخرين وتكوين الصداقات "، وفي المرتبة الثانية جاء " متابعة الأخبار والأحداث الجارية "، وهذا يدل على أن الشباب يرغبون في بناء شبكة من العلاقات الشخصية والاجتماعية، حيث توفر هذه المنصات بيئة تفاعلية تتيح لهم التواصل المستمر مع الأصدقاء والعائلة وتوسيع دائرة معارفهم، كما أنها يتيح لهم متابعة الأخبار والأحداث الجارية في الوقت الفعلي، مما يمكنهم من البقاء على اطلاع دائم بما يحدث حولهم، سواء كان ذلك في نطاق محلي أو عالمي، مما يعزز من أهمية وسائل الإعلام الجديد كأداة رئيسية لتحقيق هذين الهدفين.
- أن المبحوثين عينة الدراسة يستخدمون عدة تطبيقات ومنصات للإعلام الجديد عبر شبكة الإنترنت، وجاء في مقدمتها " مواقع التواصل الاجتماعي "، وفي المرتبة الثانية جاءت " تطبيقيات المعاملات المالية ومواقع البيع والشراء عبر الانترنت ".
- ارتفاع مستوى حرص المبحوثين عينة الدراسة على تأمين وحماية بياناتهم الشخصية عبر تطبيقات ومنصات الإعلام الجديد التي يستخدمونها، بمتوسط حسابي بلغ 2.2725، وهذا يشير إلى وعي متزايد بأهمية الخصوصية في العالم الرقمي. فيُظهر المبحوثون اهتمامًا كبيرًا باتخاذ إجراءات وقائية لحماية معلوماتهم الشخصية من المخاطر المحتملة مثل الاختراقات الأمنية أو إساءة استخدام البيانات، وهذا الحرص يعكس تفهمًا عميقًا للتحديات التي ترافق استخدام التطبيقات والمنصات الرقمية، خاصة في ظل تزايد حوادث القرصنة وتسريب البيانات، كما يشير إلى أن الشباب باتوا أكثر إدراكًا لأهمية إعدادات الخصوصية واستخدام كلمات مرور قوية وتحديثات أمنية دورية للحفاظ على سرية بياناتهم. في النهاية، يعكس هذا السلوك حرص المبحوثين على تعزيز أمانهم الرقمي وضمان تجربة آمنة عند استخدام وسائل الإعلام الجديد.

- أن المبحوثين عينة الدراسة لا يثقون بالشكل الكافي في أمان بياناتهم ومعلوماتهم عبر تطبيقات ومنصات الإعلام الجديد التي يستخدمونها، حيث جاء في المرتبة الأولى " أثق إلى حد ما "، وذلك بنسبة 54%، بينما جاءت نسبة من يثقون " تماماً "، 38.25%، في حين بلغت نسبة من " لا يثقون في ذلك "، 7.75%.

- أن اتجاه المبحوثين عينة الدراسة جاء مرتفعاً نحو مفهوم الأمن السيبراني وانتهاك الخصوصية لديهم بأنه " نشاط إجرامي يستهدف الإضرار بالأفراد والمجتمعات "، بمتوسط حسابي بلغ 2.4825، ويعكس هذا الاتجاه وعيًا قويًا بالمخاطر المرتبطة بالأنشطة السيبرانية غير القانونية، مثل الاختراقات الإلكترونية وسرقة البيانات الشخصية. يرى المبحوثون أن مثل هذه الأنشطة لا تقتصر على تهديد الأفراد فقط، بل تمتد آثارها لتشمل المجتمع ككل، حيث يمكن أن تؤدي إلى اضطرابات اجتماعية واقتصادية واسعة النطاق. يشير هذا الوعي المتزايد إلى الحاجة الماسة لتعزيز ثقافة الأمن السيبراني واتخاذ التدابير الوقائية اللازمة لحماية المعلومات والخصوصية في العالم الرقمي المتطور.

- جاءت " منصات التواصل الاجتماعي " في مقدمة مصادر معرفة المبحوثين بموضوع الأمن السيبراني، وجرائم انتهاك الخصوصية، وذلك بنسبة 74.25%، تليها في المرتبة الثانية " الأصدقاء والمعارف والأقارب " بنسبة 49%.

- أكد 80.75% من المبحوثين عينة الدراسة بأنهم لم يتعرضوا لجريمة انتهاك الخصوصية لبياناتهم عبر تطبيقات ومنصات الإعلام الجديد التي يستخدمونها، بينما نسبة 19,52%، أشاروا إلى أنهم تعرضوا لهذه الجرائم.

- أن نسبة 53.50% من المبحوثين عينة الدراسة يعلمون بأن نشر بياناتهم الشخصية دون إذن منهم يعد انتهاكاً لخصوصيتهم وفعلا مخالفا للقانون يعرض مرتكبيه للعقوبة، بينما نسبة 46.50% ليس لديهم معرفة بذلك.

- أظهر المبحوثون عينة الدراسة ايجابيتهم حال تعرضهم لاختراق خصوصيتهم عبر أحد تطبيقات ومنصات الإعلام الجديد التي يستخدمونها، حيث أكدوا أنهم سيتخذون ردود فعل نحوها، لكنها متباينة بينهم، فنسبة 52.75% من عينة الدراسة أفادت بأنها " ستقوم بإبلاغ رجال الشرطة والجهات المعنية ".

- جاء اتجاه المبحوثين عينة الدراسة نحو السلوكيات التي يتبعونها للحفاظ على بياناتهم وعدم انتهاك خصوصيتهم عبر تطبيقات ومنصات الإعلام الجديد " مرتفعاً " بصفة عامة في جميع إجاباتهم، وجاء في مقدمة هذه السلوكيات " تسجيل الخروج من الحسابات عقب انتهاء استخدامها مباشرة".

- أرجع المبحوثين عينة الدراسة انتشار جرائم انتهاك الخصوصية عبر تطبيقات ومنصات الإعلام الجديد إلى عدة أسباب، وجاء اتجاههم نحوه هذه الأسباب متوسطاً بصفة عامة، وفي مقدمة هذه الأسباب جاء " عدم اكتشاف هذه الوقائع إلا بعد فترة زمنية طويلة بما يصعب تجنبها"، وفي المرتبة الثانية جاء " عدم إبلاغ الضحايا عن تعرضهم لهذه الجريمة بما يساعد على تكرارها ".
- جاء اتجاه المبحوثين عينة الدراسة نحو دوافع انتهاك الخصوصية عبر تطبيقات ومنصات الإعلام الجديد " مرتفعاً " بصفة عامة، وقد جاء في مقدمة هذه الدوافع " تحقيق مكاسب مادية باستغلال مهارات التعامل غير الأخلاقية مع الانترنت "، وفي المرتبة الثانية جاء " الانتقام من الأشخاص والإساءة لهم والتشهير بهم ".
- تباينت اتجاهات المبحوثين عينة الدراسة نحو الأضرار والآثار السلبية لمخاطر انتهاك الخصوصية على مستوى الأفراد، فقد جاء اتجاههم " مرتفعاً " نحو ضرر " الابتزاز المادي للأفراد عبر سرقة الصور والفيديوهات "، كما جاء اتجاههم " مرتفع " أيضا نحو ضرر " الاحتيال والنصب وسرقة الأموال والحسابات البنكية ".
- جاء اتجاه المبحوثين عينة الدراسة نحو الأضرار والآثار السلبية المحتملة لمخاطر انتهاك الخصوصية على مستوى المجتمع" مرتفعاً "، في العديد من هذه الأضرار، وفي مقدمتها " سرقة الحسابات البنكية للمؤسسات بما يضر بالاقتصاد القومي "، وفي" إثارة الفوضى والفتن والاضطرابات داخل المجتمع ".
- قدم المبحوثين عينة الدراسة عدداً من المقترحات للحد من ظاهرة انتهاك الخصوصية ومكافحتها عبر تطبيقات ومنصات الإعلام الجديد، جاء في مقدمتها " التوعية الأسرية للأبناء وخاصة صغار السن بكيفية التعامل الآمن مع الانترنت" ثم في المرتبة الثانية " العمل على محو الأمية التكنولوجية في المجتمعات".

توصيات الدراسة وما تثيره من بحوث مستقبلية:

أولاً: التوصيات:

1. يجب تكثيف الحملات التوعوية الموجهة للشباب الكويتي حول أهمية الأمن السيبراني، وتوضيح المخاطر المرتبطة بانتهاك الخصوصية عبر تطبيقات ومنصات الإعلام الجديد، من خلال البرامج التعليمية، والورش التدريبية، وحملات التوعية عبر وسائل الإعلام التقليدية والرقمية.
2. ضرورة إدراج مفاهيم الأمن السيبراني وحماية الخصوصية في المناهج الدراسية بمراحل التعليم المختلفة، لضمان تنشئة جيل واعٍ بأهمية حماية بياناته الشخصية والتعامل بشكل آمن مع التكنولوجيا.
3. تشجيع الشباب الكويتي على اكتساب مهارات تقنية متقدمة في مجال الأمن السيبراني، وذلك من خلال الدورات التدريبية والشهادات المعترف بها دولياً، لتمكينهم من حماية بياناتهم بشكل فعال.
4. ضرورة التعاون مع الجهات الحكومية لتنفيذ سياسات أكثر صرامة لحماية الخصوصية، وضمان تطبيق قوانين تحمي المستخدمين من مخاطر الانتهاكات السيبرانية عبر التطبيقات والمنصات الرقمية.
5. توجيه الشباب نحو تبني ممارسات آمنة عند استخدام الإنترنت، مثل تفعيل التحقق بخطوتين، واستخدام كلمات مرور قوية، وتجنب مشاركة المعلومات الشخصية على منصات غير موثوقة.
6. تشجيع البحث العلمي في مجال الأمن السيبراني بهدف تطوير أدوات وتقنيات جديدة لحماية المستخدمين من تهديدات الخصوصية على الإنترنت، وتقديم الدعم للمشاريع المبتكرة التي تسهم في تعزيز الأمن الرقمي.
7. العمل مع منصات الإعلام الجديد لتطوير ميزات حماية خصوصية المستخدمين، وتسهيل وصول الشباب إلى أدوات التحكم في الخصوصية وضبطها بما يتوافق مع أفضل الممارسات الأمنية.

ثانياً: مقترحات لدراسات مستقبلية:

- إجراء دراسات حول دور وسائل الإعلام في توجيه الجمهور للتعامل الصحيح مع منصات وتطبيقات الإعلام الجديد، وإكسابهم مهارات وآليات حماية الخصوصية.
- إجراء دراسات تتناول كيفية توظيف الذكاء الاصطناعي في الكشف عن عمليات انتهاك الخصوصية.
- إجراء مزيد من الدراسات التي تتناول الخصوصية وآليات مواجهة انتهاكها، والعقوبات القانونية لها.
- إجراء دراسات تستهدف النخبة الإعلامية لتقديم مقترحات في كيفية رفع وعي أفرد المجتمع بمفهوم الأمن السيبراني، وأهميته على مستوى الفرد والمجتمع.

المراجع :

(1) منى عبد الله السمحان، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، **مجلة كلية التربية**، ع 11، يوليو 2020، جامعة المنصورة، كلية التربية 2020، ص 5.

(2) عبد الأمير مويت الفيصل، إسراء هاشم سيد، انتهاك الخصوصية في مواقع التواصل الاجتماعي، **مجلة الباحث الإعلامي**، ع 36، يونيو 2017، جامعة بغداد، كلية الإعلام، ص213.

(3) Mrittika Rani Dey, Bulbul Ahamed, Mohammad Rashed Hasan Polas , Empowering Students for Cybersecurity Awareness Management in the Emerging Digital Era: The Role of Cybersecurity Attitude in the 4.0 Industrial Revolution Era, **Published In SAGE Journals**, January-March 2024, Volume 14, Issue 1, https://0c113y2m3-1105-y-https-doi-org.mplbci.ekb.eg/10.1177/21582440241228

(4) مطلق سعد العميري، استراتيجيات الإعلام الإلكتروني في الكويت تجاه الأمن السيبراني، **المجلة العربية للعلوم الإنسانية**، مج42 ،ع165 ، 2024، جامعة الكويت - مجلس النشر العلمي، 2024، ص 11:42.

(5) Anakha Prakash , Sanju R, The Effectiveness of Using Social Media to Raise Cyber Safety Awareness Among the Public ،**Journal of the Asiatic Society of Mumbai**, 2024, Vol. XCVII, No.02.

(6) Mengqi Liao, Jinping Wang, Cheng Chen, S Shyam Sundar, Less vigilant in the mobile era? A comparison of information processing on mobile phones and personal computers, New Media & Society, First published online November 30, 2023, https://0c113rlw0-1106-y-https-doi-org.mplbci.ekb.eg/10.1177/14614448231209475

(7) هدير محمود عبد الله أحمد، العلاقة بين معرفة مستخدمي الانترنت بسياسات وإجراءات أمن المعلومات وسلوكيات حماية أمنهم السيبراني، **المجلة المصرية لبحوث الإعلام**، المجلد 2023، العدد 82 ، الجزء الثاني يناير 2023، جامعة القاهرة، كلية الإعلام، ص 599-639.

(8) شيرين عبد الحفيظ عبد القادر، دور الإعلام الرقمي في تعزيز الأمن السيبراني ومكافحة التهديدات والجرائم السيبرانية، **المجلة العلمية لبحوث العلاقات العامة والإعلان**، ع 25، يونيو 2023، جامعة القاهرة، كلية الإعلام، قسم العلاقات العامة والإعلان، ص 47: 85.

(9) أماني حمدي قرني، إيمان عبد المنعم خطاب، دور مواقع الإعلام الرقمي في حماية الأمن السيبراني: دراسة تحليلية لعينة من المواقع الخاصة بالأمن السيبراني، **المجلة المصرية لبحوث الإعلام**، ع 80، مايو 2022، جامعة القاهرة ، كلية الإعلام، ص 657: 687.

(10) بشائر حامد عبد القادر، أمال سعد الدين حسين، دور الصحف السعودية في تنمية الوعي بالأمن السيبراني : دراسة على القائم بالاتصال، **المجلة العربية للإعلام والاتصال**، ع 25، مارس 2021، الجمعية السعودية للإعلام والاتصال، ص 295: 335.

(11) Nnamdi O. Madichie, Ali Tarhini, Nisreen Ameen, Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce, Computers in Human Behavior , jan 2021,vol 114(6), https://doi.org/10.1016/j.chb.2020.1065

(12) آية طارق عبد الهادي، إدراك مستخدمي مواقع التواصل الاجتماعي لأهمية الأمن السيبراني و دوره في الأمن المعلوماتي : دراسة ميدانية، **المجلة المصرية لبحوث الإعلام**، المجلد 2، العدد 77، ج. 3، ديسمبر 2021، جامعة القاهرة، كلية الإعلام ، ص 649:701.

(13) نهي مجدي محمد السيد، الأمن السيبراني وعلاقته بالمضمون الإعلامي في ظل رؤية مصر 2030، **المجلة العربية لبحوث الإعلام والاتصال**، المجلد 2021، العدد 35 ، ديسمبر 2021، جامعة الأهرام الكندية، كلية الإعلام، ص484-514.

(14) Kleij, R. van der, Hoff-De Goede, S. van 't, Weijer, S. van de, Leukfeldt, R, How Safely Do We Behave Online? An Explanatory Study into the Cybersecurity Behaviors of Dutch Citizens , Springer International Publishing, Advances in Human Factors in Robots, Unmanned Systems and Cybersecurity Lecture Notes in Networks and Systems, 2021, p. 238-246.

(15) أسماء أحمد أبو زيد، استراتيجيات خطاب صحافة التكنولوجيا العربية تجاه الأمن السيبراني: دراسة تحليلية مقارنة، **المجلة المصرية لبحوث الرأي العام**، مج20 ،ع2، يونيه 2021، جامعة القاهرة، كلية الإعلام، مركز بحوث الرأي العام، ص 1:43.

(16) مجدي الداغر، اتجاهات النخبة نحو توظيف الإعلام الأمني لتطبيقات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية وانعكاساته على دعم وتعزيز الأمن السيبرانى في مصر: دراسة ميدانية، **المجلة العربية لبحوث الإعلام والاتصال**، المجلد 2021، العدد 33، يونيو 2021، جامعة الأهرام الكندية، كلية الإعلام، ص 4-110

(17) Jose Niño Sales, Ryan Tiongco, Simin Lu, Mary Jane Ruiz, Jocelyn Cruz , Maricar Prudente, Personal privacy and cyber security: Student attitudes, awareness, and perception on the use of social media, nternational Journal of Curriculum and Instruction16(1) (2024) 175-190

(18) ريم المرموم، تصور الطلبة للخصوصية في شبكات التواصل الاجتماعي في دولة الإمارات العربية المتحدة، **المجلة المصرية لبحوث الإعلام**، المجلد 2024، العدد 87، إبريل 2024، جامعة القاهرة، كلية الإعلام، ص 63-97

(19) زينب عبد العظيم عبد الواحد، استخدام المراهقين لشبكة الفيس بوك وعلاقته بقلق الابتزاز الالكتروني لديهم، **مجلة البحوث الإعلامية**، مجلد 63 ،عدد 3 ، أكتوبر 2023، جامعة الأزهر، كلية الإعلام، 2023.

(20) ياسمين محمد كمال وآخرون، تعرض الشباب الجامعي للجرائم الالكترونية عبر مواقع التواصل الاجتماعي ومستوى الوعي بخطورتها، **المجلة العلمية لكلية التربية النوعية**، جامعة دمياط، المجلد 2023، العدد 8 ، ديسمبر 2023، ص 119: 145.

(21) Rocheleau, Jessica ,and Sonia Chiasson (2022),Privacy and Safety on Social Networking Sites: Autistic and Non-Autistic Teenagers' Attitudes and Behaviors , ACM Transactions on Computer-Human Interaction (TOCHI), Volume 29, Issue 1, Article No.: 1, pp 1 – 39.

(22) Thilini B. G. Herath, Prashant Khanna, Monjur Ahmed, Cybersecurity Practices for Social Media Users: A Systematic Literature Review, Journal of Cybersecurity and Privacy, January 2022, 2(1):1-18.

(23) ولاء محمد محروس، ياسر محمد الناغي، إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق (deep fake) وعلاقته باستخدامهم الآمن لتلك المواقع، **المجلة العلمية لبحوث الصحافة**، ع 24، ديسمبر 2022، جامعة القارة، كلية الإعلام ، قسم الصحافة ، ص 383: 425.

(24) Sophie C. Boerman, Sanne Kruikemeier, and Frederik J. Zuiderveen Borgesius, Exploring Motivations for Online Privacy Protection Behavior: Insights From Panel Data, Communication research, Volume 48 Issue 7, October 2022, pp. 953-977.

(25)هاني إبراهيم محمد، اتجاهات الشباب الجامعي نحو انتهاك الحياة الخاصة عبر شبكات التواصل الاجتماعي وآليات حماية الخصوصية: دراسة ميدانية، **مجلة البحوث والدراسات الإعلامية**، ع 20، يونيو 2022، المعهد الدولي العالي للإعلام بالشروق، ص 273: 349.

(26) Ralf De Wolf, Contextualizing how teens manage personal and interpersonal privacy on social media, new media & society, Volume 22 Issue 6, June 2020, pp 1058–1075.

(27) سمير محمد حسين، **الرأي العام، الأسس النظرية والجوانب المنهجية**، ط1 (القاهرة، عالم الكتب، 1997) ص 131.

(28) تم تحكيم الاستمارة من السادة الأساتذة الآتي أسمائهم:

- أ.د/ مناور الراجحي، عضو هيئة تدريس – جامعة الكويت.
- د/ محمد الشمري، عضو هيئة تدريس – أكاديمية سعد العبد الله للعلوم الأمنية وزارة الداخلية.
- د/ مطلق المطيري، عضو هيئة تدريس أكاديمية سعد للعلوم الأمنية وزارة الداخلية.

(29) Petronio, S. (2002). Boundaries of privacy: Dialectics of disclosure. Suny Press,P. 1

(30) Ralf De Wolf, 2020,Contextualizing how teens manage personal and interpersonal privacy on social media, op cit, p 1060.

(31) Petronio, S. (2002). Op cit ,P 2.

(32) Jeffrey T. Child, Blogging Privacy Rule Orientations, Privacy Management, and Content Deletion Practices: The Variability of Online Privacy Management Activity at Different Stages of Social Media Use. Computers in Human Behavior, V 28. No 5, p 1872.

(33) التقرير الصادر عن الاتحاد الدولي للاتصالات حول اتجاهات الإصلاح في الاتصالات لعام 2010 - 2011.

(34) منى الأشقر، **الأمن السيبراني التحديات ومستلزمات المواجهة**، المركز العربي للبحوث القانونية والقضائية، مايو، 2012، ص16.

(35) أديب أحمد، تأثير تكنولوجية الاتصال في الأنواع الصحفية للصحافة الإلكترونية، **مذكرة ماجستير**، كلية العلوم السياسية والإعلام، جامعة الجزائر بن يوسف بن خدة 2010، ص08

(36) بعوني ليلى، التهديدات في الفضاء السيبراني وانعكاساتها على السيادة الرقمية: القرصنة الالكترونية نموذجا، **مجلة استراتيجيا**، ع 16، المعهد العسكري للوثائق والتقويم والاستقبالية، 2021، ص12.

(37) نائلة عادل، جرائم الحاسب الاقتصادية، دراسة نظرية تطبيقية، القاهرة، دار النهضة العربية، ص. 45.

(38) سميرة عابد، انتهاك الحق في الخصوصية عبر شبكة التواصل الاجتماعي.. دراسة مقارنة، **مجلة معارف**، المجلد18، ع1، يونيو 2023، جامعة باجي مختار، الجزائر، ص 112.

(39) أحمد ماجد، **الذكاء الاصطناعي بدولة الإمارات**، دبي: إدارة الدراسات والسياسات الاقتصادية، وزارة الاقتصاد، الإمارات العربية المتحدة، 2018، ص 4.

(40) مركز هردو لدعم التعبير الرقمي، **انتهاك الخصوصية الرقمية في الصحافة: المهنية الصحفية والحياة الشخصية**، القاهرة، 2017، ص5.

(41) ريم المرموم، تصور الطلبة للخصوصية في شبكات التواصل الاجتماعي في دولة الإمارات العربية المتحدة، **مرجع سابق**.

(42) Sophie C. Boerman, Sanne Kruikemeier, and Frederik J. Zuiderveen Borgesius, Exploring Motivations for Online Privacy Protection Behavior: Insights From Panel Data. **Op.cit.**

(43) هاني إبراهيم محمد، اتجاهات الشباب الجامعي نحو انتهاك الحياة الخاصة عبر شبكات التواصل الاجتماعي وآليات حماية الخصوصية: دراسة ميدانية، **مرجع سابق**.

(44) Anakha Prakash , Sanju R, THE EFFECTIVENESS OF USING SOCIAL MEDIA TO RAISE CYBER SAFETY AWARENESS AMONG THE PUBLIC, **Op.cit.**

(45) هدير محمود عبد الله أحمد، العلاقة بين معرفة مستخدمي الانترنت بسياسات وإجراءات أمن المعلومات وسلوكيات حماية أمنهم السيبراني، مرجع سابق.

(46) Mrittika Rani Dey, Bulbul Ahamed, Mohammad Rashed Hasan Polas ,Empowering Students for Cybersecurity Awareness Management in the Emerging Digital Era: The Role of Cybersecurity Attitude in the 4.0 Industrial Revolution Era, **Op.cit.**

(47) نهي مجدي محمد السيد، الأمن السيبراني وعلاقته بالمضمون الإعلامي في ظل رؤية مصر 2030، **مرجع سابق.**