المملكة العربية السعودية

جامعة طيبة

قسم علم معلومات ومصادر التعلم

بحث بعنوان:

حماية البيانات الشخصية في وسائل تكنولوجيا المعلومات: دراسة تحليلة

إعداد الطلاب:

خالد لافي الحجيلي

410 0011

عبد الله سلطان المغذوي

4101608

عبد المجيد نقاء الحربي

4100209

فيصل بخيت الجهني

4106663

نواف مبشر الجهني

4100230

إشراف الأستاذ الدكتور:

أسامة حامد


بسم الله الرحمن الرحيم

ملخص الدراسة

هدفت هذه الدراسة إلى التعرف على الانتهاكات التي تتعرض لها البيانات الشخصية في التكنولوجيا المعلوماتية، تحديد أهم الوسائل التي تستخدم من لحماية البيانات الشخصية في التكنولوجيا المعلوماتية، ولتحقيق هدف الدراسة تم تصميم أداة الاستبانة كأداة لجمع البيانات، والتي تم توزيعها على عينة من مجتمع الدراسة البالغ عددهم (153) طالب وطالبة في جامعة طيبة، كما اتبعت الدراسة المنهج الوصفي التحليلي في إجراء هذا البحث، وتوصلت إلى عدد من النتائج، ومنها:

- بينت نتائج الدراسة بأن أفراد عينة الدراسة يستخدمون العديد من الوسائل الخاصة بتكنولوجيا المعلومات ومنها الأجهزة الذكية والحواسيب.
- أظهرت النتائج أن الأفراد يحرصون على حماية البيانات الشخصية بشكل مستمر.
- يتم استخدام العديد من الطرق في حماية البيانات الشخصية ومنها استخدام كلمات مرور قوية وتغييرها بشكل دوري، واستخدام تقنية التشفير، وعدم النقر بروابط مشبوهة، وتجنب مشاركة البيانات الشخصية مع مصادر غير موثوقة.

وفي ضوء النتائج السابقة، أوصى البحث بمجموعة من التوصيات ومنها:

- لابد من تحليل وتقييم التهديدات المحتملة للبيانات الشخصية والمعلومات الحساسة المخزنة في الأنظمة.
- وضع سياسات أمان صارمة تغطي مجموعة متنوعة من الجوانب مثل كلمات المرور القوية وسياسات التحقق من الهوية والوصول المشروط وتشفير البيانات وغيرها.

جدول المحتويات

فهرس الجداول

الفصل الأول: الإطار العام للدراسة

المقدمة

إنّ التطور التكنولوجي الهائل أدى إلى توليد بيانات ضخمة للمستخدمين، كما أنّ هذا الكم الهائل من البيانات العامة والخاصة عن المستخدمين وتفاعلاتهم إلى خلق ثورة جديدة، حيثُ تستخدم الشركات والمنظمات الربحية والغير ربحية والخاصة والحكومية بالعديد من الطرق، حيثُ يتوقف مسار اتخاذ القرارات في هذه الشركات والمنظمات على البيانات المولدة، حيثُ أنّه ليس بالضرورة أن تعود استخدام البيانات الشخصية بالنفع على الأفراد، ليس بالضرورة أيضاً أنْ يكون استخدامها ملموساً وظاهراً للعيان، وهنا تظهر مخاطر امتلاك والسيطرة على هذه البيانات. تجمع غالبية البيانات، دون ملاحظة أو موافقة صاحبها، وفي غالبية الأحيان تشمل هويتهم ومعلوماتهم الشخصية ومن ثم بعد ذلك تحفظ وتؤرشف وتستخدم حسب حاجة مالكها. وهذا ما يجعل الأفراد عرضة لمخاطر لا بد منها، في ظل غياب قانون يحميهم ويحمي خصوصيتهم، من جامعي البيانات. (أبو عرقوب، 2021).

وتقتضي خصوصية البيانات تنظيم عملية جمع البيانات والمعلومات الشخصية ومعالجتها واستخدامها ونقلها على نحو يكفل سريتها خصوصاً في ظل المخاطر المتزايدة للكشف عنها وإساءة استخدامها بفعل تكنولوجيا المعلومات والتطور المتعاظم في أنظمة الذكاء الاصطناعي، ويعتبر الحق في حماية البيانات الشخصية وصونها وعدم إفشائها للغير من أهم وأعظم صور الحق في الخصوصية أو حرمة الحياة الخاصة فالحفاظ على أسرار الشخص هو جوهر وأساس وضمان حرية الخصوصية ضد انتهاك الغير. (عبد الحميد، 2020)

إلا أنّ التطورات الحديثة في مجال تكنولوجيا المعلومات باتت تهدد الخصوصية وتقلل من مقدار السيطرة على البيانات الشخصية وتفتح المجال أمام إمكانية حدوث مجموعة من العواقب السلبية نتيجة الوصول إلى تلك البيانات، وقد شهد النصف الثامن من القرن العشرين وضع نظم لحماية البيانات، وذلك استجابة لزيادة مستويات معاجلة البيانات الشخصية، و أصبح القرن الحادي والعشرون قرن البيانات الضخمة وتكنولوجيا المعلومات المتقدمة، فضلاً عن ظهور شركات التكنولوجيا العملاقة واقتصاد المنصات الرقمية، الذي يتزامن مع تخزين البيانات بحجم الاكسابايت ومعاجلتها. (الشبيلي، 2020).

مشكلة الدراسة

أصبحت تكنولوجيا المعلومات من لوازم الحياة الضرورية في عصر التكنولوجيا والأقمار الصناعية لما توفره من مميزات للمستخدمين فمن خلالها جعلت العالم بمثابة القرية الكونية الصغيرة التي تلاشت حدودها وتقاربت شعوبها، حيثُ أنّها أصبحت مسرح خصب للجرائم الخاصة بانتهاك الخصوصية والاعتداء على البيانات الشخصية (مسعد، 2018)، وتتبع مشكلة البحث بالإجابة عن التساؤل الرئيسي:

كيف تتم حماية البيانات الشخصية في تكنولوجيا المعلوماتية؟

تساؤلات الدراسة

ولا شك أنّه يتفرع عن هذه الإشكالية العديد من التساؤلات التي تخص مشكلة الدراسة منها (الشبيلي، 2020):.

- ما طبيعة الانتهاكات التي تتعرض لها البيانات الشخصية في التكنولوجيا المعلوماتية؟

- ما طبيعة الوسائل القانونية المستخدمة من أجل حماية البيانات الخاصة بتكنولوجيا المعلومات؟
- ما أبرز الوسائل التي يتم اللجوء إليها من أجل حماية البيانات الشخصية بمجال تكنولوجيا المعلومات؟
- كيف يمكن لتكنولوجيا المعلومات أنْ تتغلب بنفسها على مخاوف الخصوصية؟

أهمية الدراسة

رافقت التطورات التي عرفتها التقنية المعاصرة وصول المعلومات والبيانات إلى كثير من شركات تكنولوجيا المعلومات في كافة بقاع الأرض وهذه الشركات قد دامت على نحو يقارب عقدين من الزمن خاضعة لتشريعات في ذاك الوقت لحماية البيانات الشخصية بصورة كافية من مخاطر انتهاك الخصوصية، إلا أنّ الأمور تتوجه في الوقت الحالي إلى فرض التزامات صارمة من أجل حماية البيانات الشخصية (طه،2019). وهذا يكتسب بحثنا أهمية كبيرة منها:

- إنّ حماية البيانات الشخصية لها أهمية كبيرة لتعلقها بكرامة الإنسان وشرفه وحقه في الحفاظ على خصوصيته التي هي حق من الحقوق الأساسية المقررة في المواثيق العالمية والإقليمية.
- تتناول هذه الدراسة موضوع حديث النشأة يتعلق بحماية البيانات الشخصية.
- خلفت ثورة تكنولوجيا المعلومات أثر عميق في جميع المجالات، ولم تعد وسائل الحماية التقليدية صالحة لمواجهة التعدي على البيانات والمعلومات الشخصية.
- تطورت البيانات الشخصية للفرد عن المعنى التقليدي نتيجة التطور العلمي الهائل لتكنولوجيا المعلومات.

- منع الوصول غير المصرح به أو استخدام البيانات الشخصية والمعدات المستخدمة في المعالجة.

أهداف الدراسة

تسعى الدراسة إلى تحقيق الأهداف التالية:

- معرفة الانتهاكات التي تتعرض لها البيانات الشخصية في التكنولوجيا المعلوماتية.
- تحديد أهم الوسائل التي تستخدم من لحماية البيانات الشخصية في التكنولوجيا المعلوماتية.
- توضيح أهم الوسائل التي يتم اللجوء إليها لكي تتم حماية البيانات الشخصية.

فرضيات الدراسة

من أجل المساهمة في الإجابة عن الإشكالية والأسئلة الفرعية نطرح الفرضيات التالية:

- لا يوجد علاقة ذات دلالة إحصائية بين طبيعة الانتهاكات التي تتعرض لها البيانات الشخصية وبين التكنولوجية المعلوماتية.
- لا يوجد علاقة ذات دلالة إحصائية بين طبيعة الوسائل القانونية المستخدمة لحماية البيانات وبين تكنولوجية المعلومات
- لا يوجد علاقة ذات دلالة إحصائية بين الوسائل التي يتم اللجوء إليها لحماية البيانات الشخصية وبين مجال تكنولوجيا المعلومات.
- لا يوجد علاقة ذات دلالة إحصائية بين تكنولوجيا المعلومات وبين مخاوف الخصوصية.

منهجية الدراسة

اعتمد الباحث في هذه الدراسة على تطبيق المنهج الوصفي التحليلي في هذه الدراسة الذي اعتمد على الاستبانة كأداة للدراسة، من أجل وصف موضوع الدراسة وصفاً شاملاً ودقيقاً وذلك من خلال جمع وإلمام البيانات حول حماية البيانات في تكنولوجيا المعلومات.

أدوات الدراسة

تعتبر أدوات الدراسة هي الطريقة التي تساعد الباحث على جمع البيانات الضرورية للدراسة والتي تساعده في إنجازها بأعلى جودة من خلال الاجابة على اسئلتها وتغطية أهدافها، حيثُ استخدم الباحث في دراسته الاستبانة فهي من أدوات الدراسة المهمة.

حدود الدراسة

الحدود المكانية: تقتصر الحدود المكانية للدراسة على مختصين في المؤسسات التعليمية.

الحدود الزمانية: تقتصر الحدود الزمانية للدراسة لعام 2022م.

الدراسات السابقة

1. دراسة (صالح، 2014). بعنوان: "الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدول الاتفاق والقانون الوطن"

إنّ هذه الدراسة تضمنت مفهوم خصوصية البيانات وكيفية معالجتها وذلك عن طريق تسليط الضوء على الحق في الخصوصية والكشف عن مخاطر التقنيات الحديثة على هذا الحق، كما أنّها تضمنت كيفية حماية البيانات الشخصية في ظل التطور التكنولوجي وثورة الاتصالات والإنترنت والتوجيهات

والمقارنة بينهما في محاولة لتحليلها بيان مدى اسهام كلٍ منهما في ايجاد الحلول المناسبة، كما أنّ الباحثة اتبعت في دراستها المنهج التحليلي المقارن في دراسة نصوص القواعد القانونية التي تتعلق بالموضوع، كما أنّ الدراسة توصلت إلى أنْ تدار أمن المعلومات والحفاظ على خصوصية البيانات قضية أخلاقية في المقام الأول وأن التشريعات العربية لم تناقش سوى حماية البرمجيات والملكية الفكرية مقارنةً بالتوجيهات الصادرة عن كافة الهيئات الدولية على الرغم من وجود مبادئ عامة في مجالات حماية البيانات الشخصية عبر الإنترنت.

2. دراسة (بساعد، 2022)، بعنوان: (حماية البيانات الشخصية للمستهلك من مخاطر الدفع الالكتروني).

هدفت هذه الدراسة إلى محاولة إظهار المشاكل التي يثيرها الدفع الإلكتروني و التي تنعكس سلباً على خصوصية المستهلك وكذا إظهار الحماية القانونية المقررة لحق المستهلك في حماية بياناته الشخصية في مختلف التشريعات الوطنية، المقارنة والدولية مع تبيان ما إذا كانت هذه الحماية كافية، كما واتبعت الباحثة المنهج الوصفي التحليلي عند الشروع بتحليل النصوص القانونية والمنهج المقارن عند الاستعانة بالنصوص القانونية المقارنة وتوصلت الدراسة إلى أنّ الحماية القانونية وحدها غير كافية لذلك لابد من تدعيمها برفع الوعي بأهمية الحفاظ على هذا النوع من البيانات.

3. دراسة (يس، والسيد، 2022). بعنوان: " الخصوصية وحماية البيانات الشخصية بالمكتبات: مراجعة علمية. المجلة الدولية لعلوم المكتبات والمعلومات"

هدفت هذه الدراسة إلى التعرف على الإنتاج الفكري حول موضوع الخصوصية وحماية البيانات الشخصية عربياً وعالمياً، كما واتبعت هذه الدراسة أسلوب المراجعة العلمية لعرض الإنتاج الفكري

الذي تناول موضوع الخصوصية وحماية البيانات الشخصية بوجه عام ومجال المكتبات والمعلومات بوجه خاص، وخلصت الدراسة بمجموعة من النتائج أبرزها اهتمام العديد من المجالات بالخصوصية وحماية البيانات الشخصية من عدة جوانب أبرزها الجانب القانوني الخاص بالتشريعات والقوانين المختلفة والجانب التقني للحماية بالإضافة إلى الدور المجتمعي لنشر الوعي بكيفية حماية البيانات الشخصية.

4. **دراسة (صبرينة، 2018). بعنوان: " الحماية القانونية للحق في الخصوصية المعلوماتية. مجلة التواصل في العلوم الإنسانية والاجتماعية"**

هناك العديد من التحديات التي تواجه حياتنا في عصرنا الحالي، وهو عصر تكنولوجيا المعلومات، تحديات جديدة ومعاصرة، تتمثل في تسريب المعلومات الشخصية وذلك من خلال بنوك المعلومات حيث تتم معالجة البيانات الشخصية في غياب رقابة على عمليات جمعها وتخزينها واستعمالها، ومواقع الويب وشبكات التواصل الاجتماعي التي تسمح بتبادل ونشر المعلومات، وما يتركه مستخدموها من بيانات شخصية عن قصد أو دونه، وصولاً إلى الرقاقات الذكية وأنظمة تحديد المواقع التي تمكن من تتبع وتحديد مواقع الأفراد، من هذا المنطلق هدفت هذه الدراسة إلى الوقوف على المقصود بالخصوصية المعلوماتية والمعطيات ذات الطابع الشخصي، والحماية القانونية التي من الواجب توافرها، من أجل مواجهة مخاطر إساءة استخدام تكنولوجيا المعلومات وضمان احترام الحق في الحياة الخاصة.

5. **دراسة (بودوشة، وشاكر، 2017). بعنوان: "حماية البيانات الشخصية في مجال التجارة الإلكترونية"**

من أهم المسائل التي يثيرها التعامل في مجال التجارة الإلكترونية مسألة حماية البيانات الشخصية، لذلك عملت الكثير من الشركات والهيئات العالمية على البحث عن الإجراءات التقنية اللازمة لتوفير الأمن والأمان لهذه البيانات بمنع الاعتداء عليها، كما كرست العديد من التشريعات الوطنية وسائل قانونية من أجل حماية حقوق المتضرر في حال وقوع الاعتداء عليها تتمثل في الدعوى الجزائية والدعوى المدنية، وهدفت هذه الدراسة إلى التعرف على أحكام خاصة تحمي البيانات الشخصية للمتعاملين في مجال التجارة الإلكترونية، والتعرف على مفاهيم قانونية جديدة تتعلق بالمعاملات المعالجة إلكترونيا، حتى ينتشر الفهم الصحيح والإدراك الجيد لخبايا مثل هذه المعاملات، واتبعت هذه الدراسة المنهج الوصفي والمنهج التحليلي، وخلصت الدراسة بجملة من النتائج أهمها: تحديد الالتزامات المقررة على عاتق مؤدي خدمات التصديق الإلكتروني فيما يتعلق بعملها الأساسي المتمثل في منح شهادة التصديق الإلكتروني.

6. دراسة (المعداوي، 2018). بعنوان: " حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي"

هدفت هذه الدراسة إلى تحديد ماهية البيانات الشخصية محل الحماية من الاعتداء عليها من خلال استغلالها في أغراض الإعلانات التجارية، وخلصت الدراسة إلى أن البيانات الشخصية هي جميع البيانات المتعلقة بالشخص الطبيعي المحدد والتي تشمل: (اسمه الأول واسم العائلة وعنوان البريد الإلكتروني وكلمة المرور والجنس وتاريخ الميلاد، وكذلك كافة المعلومات أو البيانات التي يطلبها الموقع من المستخدم الذي يرغب في التسجيل على موقع معين على شبكة الإنترنت)، كما أظهرت الدراسة كافة مظاهر وصور الاعتداء على الخصوصية المعلوماتية، وركزت هذه الدراسة على حماية

المستخدم في مواجهة المسئول عن إدارة البيانات الشخصية عبر شبكات مواقع التواصل الاجتماعي، وقد انتهيت إلى أن هناك التزامات تقع على عاتق الشخص المسئول عن معالجة البيانات الشخصية، وأن الإخلال بهذه الالتزامات من شأنه أن يرتب المسئولية التعاقدية لهذا المسئول، كما تناول البحث حماية المستخدم في مواجهة الغير المسئول عن انتهاكات خصوصية البيانات الشخصية لمستخدمي مواقع التواصل الاجتماعي، وقد استعرضت الحق في النسيان الرقمي باعتباره من الحقوق اللصيقة بالشخصية، فهو يهدف إلى حماية خصوصية مستخدمي مواقع التواصل الاجتماعي الذي قد يندمون لاحق على احداث معينة قاموا بنشرها على هذه المواقع، كما اتبعت الدراسة المنهج التحليلي المقارن من أجل تحليل النصوص المتعلقة بموضوع الدراسة، وتوصلت الدراسة إلي جملة من التوصيات منها: ضرورة عقد دورات تدريبية للقضاة من أجل التوعية بالمستجدات الحديثة على شبكة الإنترنت.

الفصل الثاني: الإطار النظري للدراسة

مفهوم البيانات الشخصية

تعرف البيانات الشخصية، حسب القانون الأوروبي للخصوصية وحماية البيانات على أنها أي معلومات ترتبط بالأفراد، نستطيع من خلالها التعرف عليهم بشكل مباشر أو غير مباشر، على سبيل المثال الاسم الإيميل، العنوان الموقع الجغرافي العرق الجنس الصورة الدين، المعتقدات، معلومات التصفح الخاصة بالمواقع الآراء السياسية، الأسماء المستعارة والكنية وكلّ ما يمكن اعتباره من البيانات الشخصية التي قد تكون طرف خيط في التعرف على هوية شخص بعينه " (يس، 2022).

وتكشف البيانات الشخصية والرقمية المتوفرة على شبكة الإنترنت أو لدى الشركات والمؤسسات والحكومات الكثير عن الأفراد وأفكارهم ونمط حياتهم وتحركاتهم وأصبح من السهل استغلال هذه البيانات لإيذائهم والإيقاع بهم والتأثير عليهم وعلى خياراتهم. فعلى سبيل المثال استغلت بعض الحكومات القمعية البيانات الشخصيّة الرقمية لصحفيين وناشطين مناهضين لها لملاحقتهم وقتلهم. ولا يقتصر استغلال البيانات على الحكومات والمؤسسات، فحتى الأفراد يمكنهم استغلال بيانات شخصية لأفراد آخرين لابتزازهم وإلحاق الضّرر بهم. لذلك، أصبح من الضروري الحرص على حماية البيانات الشخصية والرقمية لكل فرد، وتوفير الحق لهم في اختيار الجهة التي يرغبون بمشاركة معلوماتهم معها، ومن لديه حق الوصول إليها، إلى جانب المدة الزمنية، التي يمكن الاحتفاظ بها في قواعد البيانات فضلًا عن قدرة الفرد على تعديل هذه البيانات متى شاء (الضناوي، 2019).

مفهوم معالجة البيانات الشخصية

يتميز مفهوم معالجة البيانات الشخصية بالاتساع؛ بهدف تحقيق الحماية الكافية والشاملة في الجماعة الأوروبية. ويمكن تعريف معالجة البيانات الشخصية على أنها أي عملية أو مجموعة من العمليات المبرمة أو لا تستخدم الوسائل الآلية لكي تطبقها على البيانات الشخصية مثل الجمع أو التسجيل أو التنظيم أو الحفظ أو التعديل أو التصميم أو الاستخراج أو الاسترجاع أو الاستخدام أو الإحالة عن طريق الإرسال أو النشر أو أي شكل آخر من الأشكال المتاحة مثل التقريب أو الربط البيني، أو القفل أو المسح أو التدمير (خلايفة، 2019).

أشكال البيانات الشخصية

البيانات الشخصية هي أية معلومات تتعلق بشخص محدد، وتشمل العديد من الأشكال، من وبين أشكال البيانات الشخصية: (الصيادي، 2019)

- الاسم الكامل: وهو الاسم الذي يعرف به الشخص ويتم استخدامه للتعرف عليه.
- العنوان: ويشمل العنوان الحالي للشخص ومن الممكن أن يتضمن الدولة والمدينة والشارع ورقم المنزل.
- البريد الإلكتروني: وهو عنوان البريد الإلكتروني الخاص بالشخص.
- رقم الهاتف: وهو رقم الهاتف الخاص بالشخص والذي يستخدم للتواصل معه.
- تاريخ الميلاد: وهو التاريخ الذي ولد فيه الشخص.
- الجنس: ويشمل الجنس الذكر والأنثى.

- الحالة الاجتماعية: وتشمل الحالة الاجتماعية الزواج، الطلاق، الأرامل، الأعزب، العزباء وغيرها.
- الجنسية: وهي الجنسية التي يحملها الشخص.
- الصورة الشخصية: وهي صورة للشخص والتي يمكن استخدامها للتعرف عليه.

تقنيات جمع واستخدام البيانات الشخصية

أفرزت تكنولوجيا الاتصال الحديثة وشبكة الإنترنت. مجموعة من التقنيات والطرق والأساليب القادرة على جمع وتحليل واستخدام البيانات الشخصية الخاصة بالمستخدمين. ولعل التقنية الأوسع انتشارا هي ملفات تعريف الارتباط التي تتبع المستهلك عبر شبكة الإنترنت. فهي تمكن المواقع الإلكترونية من جمع المعلومات عن المستخدمين على سبيل المثال نوع الجهاز والمعالج، ورقم الـIP الخاص بالمستخدم، وطريقة الاتصال بالإنترنت والمواقع التي زارها وعدد الساعات التي يقضيها على الانترنت، طبيعة اهتماماته، وما يبحث عنه، ومشترياته الإلكترونية، بالإضافة إلى كافة المعلومات الشخصية التي يضعها المستخدم في أي استمارة تسجيل على الانترنت من أرقام بطاقات ائتمانية وهواتف وعناوين وغالبًا لا يعلم زوار المواقع الإلكترونية بذلك. كما أن المعلنين يستغلون هذه المعلومات لصالح إعلاناتهم. حيث يتم استخدامها بالعادة، من قبل أطراف ثالثة، وهو ما يحتاج إلى تنظيم شامل من قبل الجهات المختصة، لأوجه جمع واستخدام هذه البيانات (كمال، 2009).

وفي السياق ذاته، فإن استخدام الهاتف المحمول بما يحتويه من تقنيات كالتعرّف على الموقع الجغرافي ومشاركته على مواقع التواصل الاجتماعي، قد أفاد المسوّقين في توجيه الإعلانات التسويقية بشكل أساسي، حسب البيانات التي تجمعها هذه التقنية بهدف توجيه الرسائل الإعلانية المناسبة له، واختياره

كجمهور مستهدف بناء عليها. وينضاف إلى كل ذلك، وبناء على الكم من المعلومات، الذي أصبح متاحا، من خلال التقنيات الحديثة والتطور الاتصالي، سهولة اختراق المواقع الإلكترونية، وقواعد البيانات والبيانات الشخصية من خلال هجمات الهاكر المنظمة التي تستهدف أفرادا أو مؤسسات بعينها، الذي يشكل حربًا مفتوحة على قاعدة الاستفادة من الثّغرات الإلكترونية المتاحة. وتتم عادة، عبر برامج معقدة، وطرق احتيالية واختراقات للأجهزة، وكل ما هو متصل بشبكة الإنترنت. وحسب الموسوي وفضل الله فإن خرق الخصوصية على شبكة الإنترنت يمكن أن يتم من قبل ثلاث جهات أساسية: (عزي، 2015)

1. مزوّد خدمات الإنترنت، حيث باستطاعته رصد كل ما تقوم به على الانترنت مكان وزمان الدخول إلى الشبكة، المواقع التي يزورها المتصفح والأوقات، والكلمات التي جرى البحث عنها والحوارات والرسائل الإلكترونية وغيرها).
2. المواقع التي يزورها المتصفح قادرة بدورها على تحديد حركته فيها، وذلك من خلال ملفات المواقع الإلكترونية الكوكيز.
3. مخترقو شبكة الإنترنت "الهاكر"، من خلال التركيز على ثغرات المنتديات الإلكترونية، ومواقع التواصل الاجتماعي.

بعد أن تُجمع بيانات المستخدمين من قبل المؤسسات والشركات تُستغل لاستهدافهم بدقة أكثر. وهناك مؤسسات وشركات تبيع هذه البيانات لأطراف ثالثة، وهذا يقع في صلب خرق الخصوصية. وتخترق الخصوصية أيضًا على مواقع التواصل الاجتماعي، من خلال إتاحة معلومات مستخدميها الشخصية للمطورين وشركات الخدمات الرقمية، لتمكينهم من الوصول إلى تفاعلات المستخدمين، دون مراقبة

من مواقع التواصل الاجتماعي. وفي السنوات الأولى لعمل منصات التواصل الاجتماعي لم يسيطر ولم يتحكّم المستخدمون ببياناتهم الشخصية، ولم تز هذه المنصات أن هناك ضرورة الإعلام المستخدمين أيا من بياناتهم منشورة، ويستطيع الآخرون الحصول عليها، كل هذا عرّض هذه المنصات للمساءلة القانونية، وهو ما أجبرها على إدخال تعديلات لحماية البيانات، على نحو دائم إلا أنها ما زالت غير كافية (غالب، 2019).

ويشكل المستقبل الرقمي تحدّيا للخصوصية، سيّما على مواقع التواصل الاجتماعي، التي باتت تسيطر على المواقع والتطبيقات، وذلك من خلال إتاحة استعمال حساباتها للتسجيل وتعبئة البيانات الشخصية الفورية، لمواقع وتطبيقات مختلفة. إضافة لإتاحة أو بيع هذه البيانات طوعيًّا، أو الحصول عليها بأساليب القرصنة، هناك، أيضًا، موظفو معالجة البيانات الشخصية الخاصة بالعملاء والمستخدمين، الذين تُوكل إليهم مهمة البحث ومعالجة وتخزين البيانات الرقمية ما يجعلهم قادرين على انتهاك الخصوصية (فقيه، 2017).

من جهة أخرى تجمع الحكومات بيانات مواطنيها، بموجب قوانين إدارية مختلفة، تشمل تسجيلات السيارات والإقامة والضرائب، بالإضافة إلى المعلومات المالية والحالة الاجتماعية واستخدام الكهرباء والمياه وغيرها، تمكّن هذه المعلومات الجهات الحكومية تنفيذ مهامها بكفاءة، إلا أنّ الخطر وارد من كشف بيانات المواطنين والاطلاع عليها لأغراض غير شرعية وغير قانونية، من قبل الحكومات ذاتها، ومن قبل طرف ثالث (علي، 2021).

تكمن أهمية الحديث عن حماية الخصوصية والبيانات الشخصيّة، بأنّ الطرق والوسائل والأساليب التي يمكن استخدامها على شبكة الإنترنت كثيرة ومتعددة، وبعضها ما زال غير مكتشف أو مولّق، وهي

تكنولوجيا تتطوّر بالتوازي مع التطور الحاصل في تكنولوجيا وتقنيات الاتصال وشبكة الإنترنت لذلك. من الأهمية بمكان توافر الوعي بالقواعد الأساسية، التي قد تساعد في تقليل حجم المعلومات والبيانات الشخصية، التي يمكن أن يعرفها الغير عن المستخدم.

انتهاك واستغلال البيانات الشخصية

يُعد انتهاك الخصوصية واستغلال البيانات الشخصية أمرين بالغيّ الأهميّة وشديدي الخطورة، وذلك لتوافر بيانات رقمية ضخمة عن كل فرد بالقدر الذي يساعد على انتحال شخصيته، ومعرفة حالته النفسية والاقتصادية والاجتماعية وحتّى السياسية. ويمكن فهم انتهاك خصوصية البيانات على أنه الحصول على معلومات العملاء أو المستخدمين وبياناتهم والاعتداء على ما يتعلّق بغلاف الفرد الخاص، على نحو الاطلاع على الحسابات والأرصدة في البنوك، بغية إلحاق الضرر والسّرقة، أو على نحو تتبع جهات اتصال الفرد، واستغلال سلوكه للإيقاع به أو التجسّس عليه (أعزان، 2013).

علاوة على ما ذُكر فإن الخطورة كامنة أيضًا بسرية عمليات بيع وتبادل البيانات الشخصية التي لا يعلم بها أحد أو لا دليل بحوزته على انتهاكها واستغلالها، سوى من نفذها وشارك بها. وتتعرض البيانات الشخصية للاختراق عادةً عندما يتم الوصول إليها بطريقة غير مصرح بها أو عندما يتم سرقتها من الجهاز أو الشبكة المخزنة عليها. وهناك عدة طرق يمكن أن تؤدي إلى اختراق البيانات الشخصية، ومن بينها: (بطيحي، 2019)

- هجمات البرمجيات الخبيثة: يمكن أن تدخل البرمجيات الخبيثة النظام عن طريق البريد الإلكتروني، أو الملفات المصابة بالفيروسات، أو المواقع الإلكترونية الخبيثة، ومن ثم تتمكن من جمع البيانات الشخصية وإرسالها إلى المهاجمين.
- هجمات القرصنة: يمكن للقراصنة اختراق أجهزة الكمبيوتر الضعيفة أو الأجهزة التي لا تحتوي على برامج حماية كافية والوصول البيانات الشخصية التي يتم تخزينها على الأجهزة.
- الهجمات على شبكات الواي فاي العامة: يمكن للمهاجمين استخدام شبكات الواي فاي العامة الغير محمية بكلمات مرور قوية للوصول إلى الأجهزة المتصلة بها والحصول على البيانات الشخصية.
- الاحتيال الإلكتروني: يتم استخدام التصيد والتصيد بالتحويل (Phishing) الإلكتروني والتصيد بالتشغيل (Spear Phishing) وغيرها من أساليب (Whaling السابق الاحتيال الإلكتروني لاستخدام الحيل والخداع لإقناع الأفراد بالكشف عن معلومات الدخول الخاصة بهم، ومن ثم يتم استخدام هذه المعلومات للوصول إلى البيانات الشخصية.

عقوبات انتهاك واستغلال البيانات الشخصية

تختلف العقوبات التي يتم فرضها على المخترقين الذين يقومون بالاختراق غير المصرح به للبيانات الشخصية، وذلك حسب البلد والتشريعات المحلية والتعامل مع الجرائم الإلكترونية. في العديد من البلدان يعتبر اختراق البيانات الشخصية جريمة يعاقب عليها القانون بشكل صارم، وقد تشمل العقوبات العديد من العواقب القانونية مثل: (التهامي، 2011)

- السجن حيث يتم حبس المتهمين لفترات 1طويلة بناءً على ثقل الجريمة وحجم الأضرار التي سببوها.
- الغرامات المالية حيث يتم فرض غرامات مالية على المخترقين والتي يمكن أن تصل إلى ملايين الدولارات في بعض الحالات.
- الإفراج عن البيانات الشخصية: حيث يتم فرض عقوبات على المخترقين الذين يستخدمون البيانات الشخصية في التحريض أو الابتزاز أو السرقة، وقد تتم إعادة البيانات المسروقة إلى أصحابها الشرعيين.
- التعويض المالي: يمكن أن يتعين على 4المخترقين دفع تعويضات مالية إلى الأفراد أو المنظمات الذين تضرروا من الاختراق.

يجب على الأفراد والمنظمات اتخاذ الإجراءات اللازمة لحماية بياناتهم الشخصية والتأكد من تحديث البرامج الأمنية وتطبيق أفضل الممارسات في مجال الأمن الإلكتروني لتقليل خطر الاختراق وتفادي العقوبات المرتبطة به.

الالتزام بسياسة الخصوصية وحماية البيانات الشخصية

الالتزام بسياسة الخصوصية وحماية البيانات الشخصية هي أمور مهمة جدًا في العصر الرقمي الحالي، حيث إن استخدام التكنولوجيا والإنترنت يعرض البيانات الشخصية للخطر. وبالتالي، فإن الشركات والمؤسسات والأفراد على حد سواء يجب أن يتبعوا بعض الإجراءات لحماية البيانات الشخصية والالتزام بسياسات الخصوصية وتشمل هذه الإجراءات: (العجمي، 2023)

1. وضع سياسة خصوصية صارمة: يجب على المؤسسات والشركات والمواقع الإلكترونية وضع سياسات خصوصية صارمة وواضحة للتأكد من أن البيانات الشخصية تتم حمايتها بشكل كافي.
2. تحديث البرامج الأمنية بشكل دوري: يجب تحديث البرامج الأمنية بشكل دوري وتنفيذ التحديثات اللازمة لتأمين الأجهزة والشبكات والمواقع الإلكترونية.
3. تشفير البيانات: يجب تشفير البيانات الحساسة والشخصية المخزنة على الأجهزة أو المرسلة عبر الإنترنت لحمايتها من الوصول غير المصرح به.
4. عدم الكشف عن المعلومات الشخصية: يجب عدم الكشف عن المعلومات الشخصية لأي شخص آخر، سواء كانت البيانات الشخصية مخزنة على الأجهزة الشخصية أو المؤسسات.
5. تدريب الموظفين: يجب تدريب الموظفين على كيفية حماية البيانات الشخصية وتنفيذ سياسات الخصوصية، وتشمل هذه الدورات توعية الموظفين حول مخاطر البريد الإلكتروني الخبيث. والهجمات الإلكترونية الأخرى.
6. تقييم الأمن السيبراني: يجب تقييم الأمن السيبراني بشكل دوري واختبار الأنظمة والشبكات وتحديث الأجهزة القديمة والتأكد من أنها تلبي المعايير الأمنية الحالية.

قوانين الخصوصية وحماية البيانات عالمياً

بحسب بيانات مؤتمر الأمم المتحدة للتجارة والتطوير، فإنّ 128 دولة من أصل 194 دولة أقرّت قوانين أو تتداول إقرار قوانين لحماية الخصوصيّة والبيانات الرقمية، كما ويشكّل القانون العام للاتّحاد الأوروبي، الخاص بالخصوصيّة وحماية البيانات الشخصيّة (GDPR)، الذي سُنّ في العام 2018،

إطارًا إيجابيًّا لحماية المستخدمين والأفراد، على استعادة السيطرة على معلوماتهم الشخصيّة والرقمية، حيث يعدّ هذا القانون الأكثر شمولًا، وقد أصبح مصدر إلهام للكثير من الحكومات والجهات التشريعية والقانونية (مشعل، 2017).

كما يشدّد القانون الأوروبي لحماية البيانات، على أنّ أحد المحاور الأساسيّة، للخصوصيّة وحماية البيانات، بعد تقييد عملية جمع البيانات هو مرحلة معالجة البيانات، حيث عرّفها على أنها أيُّ معالجة أو عملية، تنفّذ على المعلومات الشخصيّة، سواء كانت مؤتمتة من خلال برامج وخوارزميات أو يدوية، وهو ما يشمل عملية (جمع، تحليل، تسجيل، تنظيم، تقسيم، تصنيف، استخدام، مسح) لبيانات المستخدمين/الأفراد الرقميّة، الذين قد يكونون عملاء أو مستخدمين، أو زوّارًا للموقع الإلكترونيّ. بالإضافة إلى ضرورة معرفة مَن الشّخص، الذي يحقّ له الاطّلاع على البيانات ومعالجتها، وتحديد صلاحيّاته بشكل واضح ومعلوم، وإن كان موظفًّا أو مالكًا لبيانات المستخدمين، أو طرفا ثالثًا، يدير هذه البيانات، بشكل قانوني وآمن (العكيلي، 2022).

أدوات حماية البيانات الشخصية في تكنولوجيا المعلوماتية

تحتوي تكنولوجيا المعلومات على العديد من الأدوات والتقنيات التي يمكن استخدامها لحماية البيانات الشخصية ومن بين هذه الأدوات: (الموسوي وفضل الله،2013)

1. التشفير: يتم استخدام التشفير لتحويل البيانات الشخصية إلى شكل غير قابل للقراءة لحمايتها من الاختراق والوصول غير المصرح به.

2. الحماية بكلمة المرور: يمكن استخدام كلمات مرور قوية ومعقدة لحماية البيانات الشخصية، ويجب تغييرها بانتظام وعدم مشاركتها مع أي شخص آخر.
3. البرامج الحماية: يتم استخدام البرامج الحماية مثل برامج مكافحة الفيروسات وبرامج الجدار الناري لحماية البيانات الشخصية ومنع الوصول غير المصرح به.
4. التحديثات الأمنية: يجب تحديث البرامج والتطبيقات الأمنية بانتظام لتصحيح أي.. ثغرات أمنية وحماية البيانات الشخصية.
5. الحد من الوصول: يجب تقييد الوصول إلى البيانات الشخصية ومنح الوصول فقط للأشخاص المصرح لهم.
6. النسخ الاحتياطي: يجب إنشاء نسخ احتياطية للبيانات الشخصية وتخزينها في. مكان آمن لضمان عدم فقدانها أو تلفها.
7. الالتزام بسياسات الخصوصية: يجب على المنظمات والأفراد الالتزام بسياسات الخصوصية وتطبيق القوانين المتعلقة بحماية البيانات الشخصية.
8. استخدام المصادقة ذات العوامل المتعددة: قم بتمكين المصادقة ذات العوامل المتعددة (MFA) في حساباتك الشخصية عندما يتوفر هذا الخيار. هذا يضيف طبقة إضافية من الحماية عند تسجيل الدخول، حيث يتطلب منك إدخال رمز أو تأكيد عبر جهاز آخر مثل هاتفك المحمول.
9. استخدم خدمات VPN: يمكن استخدام شبكة خاصة افتراضية (VPN) لتشفير حركة البيانات الخاصة بك وإخفاء عنوان IP الخاص بك عند التصفح عبر الإنترنت، وهذا يعزز الخصوصية ويمنع الجهات الخارجية من تتبع نشاطك عبر الإنترنت (داود، 2017).

بشكل عام، يجب توخي الحذر واتخاذ الإجراءات اللازمة لحماية البيانات الشخصية وتقليل خطر تعرضها للاختراق والاستغلال غير المصرح به.

مهام موظّفو معالجة البيانات الشخصيّة الخاصة بالعملاء والمستخدمين

يقوم موظفو معالجة البيانات الشخصية للعملاء والمستخدمين بمجموعة من المهام الهامة لضمان حماية البيانات واحترام الخصوصية، ومن أهم هذه المهام ما يلي (اللمكية وآخرون، 2015):

- **جمع البيانات:** يقومون بجمع البيانات الشخصية للعملاء والمستخدمين من مصادر مختلفة، مثل استمارات التسجيل، والطلبات الإلكترونية، والمحادثات عبر الهاتف أو البريد الإلكتروني.
- **تحليل البيانات:** يقومون بتحليل البيانات المجمعة للحصول على رؤى وتحليلات قيمة تساعد في تحسين الخدمات وتلبية احتياجات العملاء والمستخدمين.
- **حفظ البيانات بشكل آمن:** يتعين على هؤلاء الموظفين الحفاظ على سرية وسلامة البيانات الشخصية المجمعة، حيث يجب أن يتم تنفيذ إجراءات أمنية قوية لحماية البيانات من الوصول غير المصرح به والاستخدام غير القانوني.
- **تنفيذ سياسات الخصوصية:** يجب على موظفي معالجة البيانات الشخصية الالتزام بسياسات الخصوصية المعمول بها في المؤسسة أو المنظمة التي يعملون فيها، كما يجب أن يكونوا على دراية بقوانين حماية البيانات المعمول بها وضمان الامتثال لها.
- **توفير حقوق العملاء والمستخدمين:** يجب على موظفي معالجة البيانات الشخصية التعامل مع طلبات العملاء والمستخدمين المتعلقة بالبيانات الشخصية، مثل طلبات الوصول أو تعديل

أو حذف البيانات، كما يجب أن يتم التعامل مع هذه الطلبات بسرعة وفقًا للقوانين واللوائح ذات الصلة.

- **التدريب والتوعية:** يجب توفير التدريب اللازم لموظفي معالجة البيانات الشخصية لزيادة الوعي بأفضل الممارسات في حماية البيانات الشخصية والخصوصية، كما ينبغي أن يكونوا على دراية بالتهديدات الأمنية والطرق الصحيحة للتعامل مع البيانات الشخصية.

حماية البيانات الشخصية عبر مواقع التواصل الاجتماعي

يعتبر حماية البيانات الشخصية عبر مواقع التواصل الاجتماعي أمراً مهماً، حيث يحتوي الحساب على معلومات شخصية قد تكون حساسة، ومن أهم الإجراءات المتخذة لحماية البيانات الشخصية ما يلي (أحمد، 2017):

- تعديل إعدادات الخصوصية: قم بزيارة إعدادات الخصوصية في حسابك على موقع التواصل الاجتماعي وتعديلها وفقاً لتفضيلاتك الشخصية، حيث أنه قد تتيح لك هذه الإعدادات تحديد من يمكنه رؤية منشوراتك ومعلوماتك الشخصية. يمكنك تقليل الوصول العام للمعلومات أو تقييدها للأشخاص المعروفين فقط.
- تجنب مشاركة المعلومات الحساسة: تذكر أن مواقع التواصل الاجتماعي تعتبر منصة عامة، وبالتالي يجب أن تكون حذراً بشأن المعلومات التي تشاركها، وتجنب مشاركة المعلومات الحساسة مثل رقم الهوية الوطنية، رقم الضمان الاجتماعي، معلومات المالية أو أي معلومات شخصية أخرى قد يستغلها الآخرون بطرق غير مرغوب فيها.

- التعامل مع الروابط بحذر: قبل النقر على رابط مرسل عبر موقع التواصل الاجتماعي، تحقق من مصدره ومصداقيته، حيث يمكن أن تحيل الروابط المشبوهة إلى صفحات ضارة أو تستغل في عمليات احتيال. استخدم الحذر والحكمة عند فتح الروابط وتأكد من أنها آمنة قبل الاستمرار.
- استخدم كلمة مرور قوية: قم بإنشاء كلمة مرور قوية لحسابك على موقع التواصل الاجتماعي. يفضل أن تكون الكلمة المرور طويلة وتحتوي على مزيج من الأحرف الكبيرة والصغيرة والأرقام والرموز. تجنب استخدام كلمات المرور الضعيفة أو السهلة التوقع مثل "123456" أو "password".
- التحقق من البرامج الضارة والاحتيال: قد تواجه برامج ضارة ورسائل احتيالية عبر مواقع التواصل الاجتماعي. كن حذرًا من الرسائل المشبوهة التي تحتوي على طلبات غريبة أو تحاول إغرائك بالمشاركة في أنشطة غير آمنة.
- تحديث التطبيقات والبرامج: تأكد من تحديث تطبيقات مواقع التواصل الاجتماعي وبرامج الأمان على أجهزتك بشكل منتظم، حيث يتم تحديثات البرامج عادةً لإصلاح الثغرات الأمنية وتعزيز الحماية. تأكد من تشغيل التحديثات التلقائية إذا كانت متاحة (عبد ربة، 2018).
- التحقق من الجهات الثالثة والتطبيقات: قبل توفير إذن لتطبيق أو خدمة طرف ثالث للوصول إلى حسابك على موقع التواصل الاجتماعي، تأكد من مصداقيته وسمعته.

- استخدم خيارات المصادقة ذات العاملين المزدوج: قد يوفر موقع التواصل الاجتماعي خيارات المصادقة ذات العاملين المزدوج، مثل إرسال رمز التحقق إلى هاتفك المحمول قبل تسجيل الدخول. قم بتمكين هذا الخيار لزيادة الحماية والتحقق من هوية المستخدم.
- مراجعة وإزالة المحتوى غير المرغوب فيه: قم بمراجعة المشاركات القديمة على حسابك على موقع التواصل الاجتماعي وتأكد من أنه لا يوجد محتوى قديم يمكن استغلاله.
- التوعية والتحسين المستمر: استمر في متابعة أحدث الممارسات والتطورات في حماية البيانات الشخصية على مواقع التواصل الاجتماعي.

الفصل الثالث: منهجية الدراسة وإجراءاتها

منهج الدراسة

يدور موضوع الدراسة حول حماية البيانات الشخصية في تكنولوجيا المعلوماتية، حيث أن هذا الموضوع يعتبر من المواضيع الهامة والتي تحتاج إلى وصف وتفسير وتحليل شامل، وكذلك التطرق إلى كافة جوانبه وتحليله كماً وكيفياً، ومن أجل ذلك اتبع الباحثين في هذه الدارسة المنهج الوصفي التحليلي لأهم ما جاء في الكتب والمراجع والدراسات إذ أنه يعتبر من أكثر مناهج البحث ملائمة للإحاطة بكافة أبعاد الدراسة، ويهدف كذلك إلى توضيح مضمون المفاهيم الأساسية في الموضوع محل الدراسة وتوضيح العلاقة الموجودة بين متغيري موضوع البحث، والوصول إلى نتائج واستنتاجات يمكن تفسيرها بطريقة كمية، وأيضاً وضع مجموعة من التوصيات والقضايا العلمية.

مصادر جمع المعلومات

استخدم الباحثين مصدرين أساسيين للمعلومات:

1. **المصادر الأولية:** وتم استخدام هذه المصادر من أجل معالجة الجوانب التحليلية لموضوع الدراسة، حيث أن الباحثين لجئوا إلى جمع البيانات الأولية من خلال استخدام الاستبانة كأداة رئيسة للدراسة، والتي صممت خصيصاً لهذا الغرض.
2. المصادر الثانوية: اتجه الباحثين إلى معالجة الإطار النظري للدراسة من خلال مصادر البيانات الثانوية المتمثلة في الكتب والمراجع العربية والأجنبية ذات العلاقة، وكذلك الدوريات

والمقالات والتقارير، والأبحاث والدراسات السابقة التي تناولت موضوع الدراسة، والمطالعة في مواقع الانترنت المختلفة.

مجتمع وعينة الدراسة

يتكون مجتمع الدراسة من طلبة جامعة طيبة، وتم اختيار عينة عشوائية بسيطة بالطريقة الطبقية العشوائية لتمثيل مجتمع الدراسة، وتتمثل عينة الدارسة في (153) طالب وطالبة من طلبة جامعة طيبة، وذلك وفق استجابات أفراد مجتمع الدراسة.

خصائص عينة الدراسة

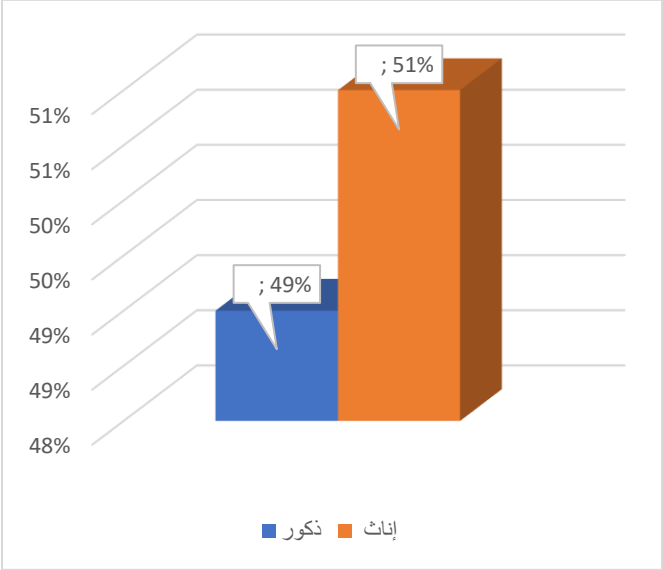
يبين الجدول الأول توزيع مفردات العينة وفقاً للبيانات الشخصية للمشمولين بالاستبيان.

1. **الجنس:**

جدول 1: توزيع عينة الدراسة وفقاً للجنس

المتغير	الصنف	العدد	النسبة المئوية
الجنس	ذكر	75	49%
	أنثى	78	51%
المجموع		153	100%

يوضح الجدول السابق رقم (1) أن غالبية أفراد عينة الدراسة من الإناث، حيث بلغت نسبتهم 51%، بينما كانت نسبة الذكور 49%.

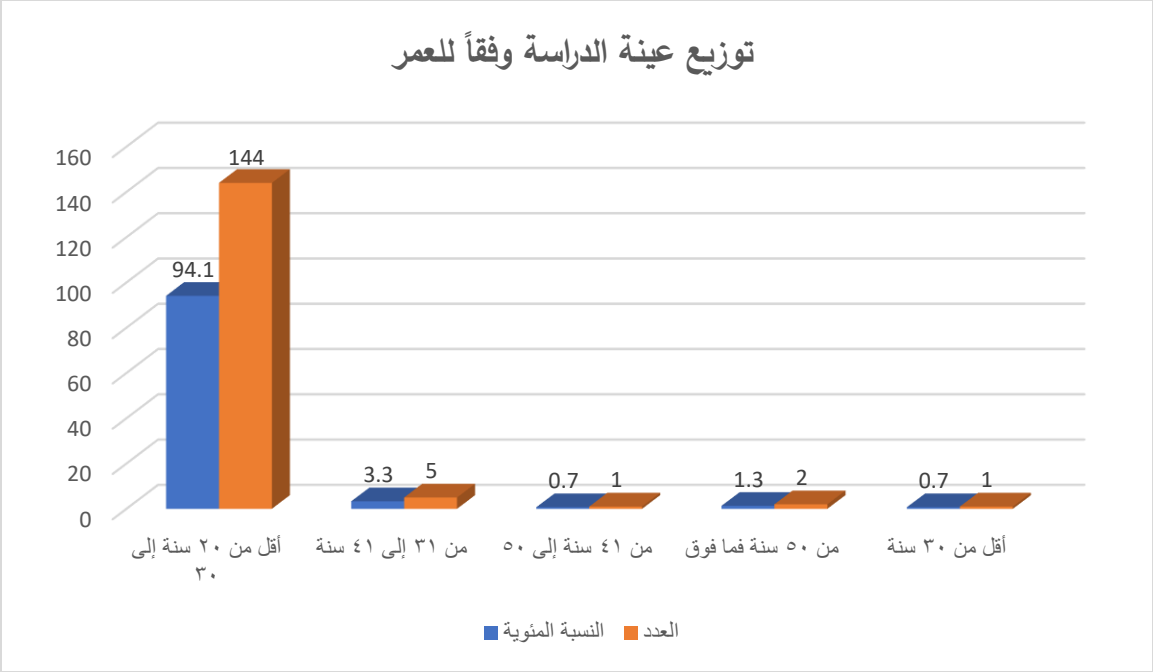


2. **العمر:**

جدول 2: توزيع عينة الدراسة وفقاً للعمر

المتغير	الصنف	العدد	النسبة المئوية
العمر	أقل من 20 سنة إلى 30	144	94.1%
	من 31 إلى 41 سنة	5	3.3%
	من 41 سنة إلى 50	1	0.7%
	من 50 سنة فما فوق	2	1.3%
	أقل من 30 سنة	1	0.7%
المجموع		153	100%

يوضح الجدول السابق رقم (2) أن غالبية أفراد عينة الدراسة أعمارهم من أقل من 20 سنة إلى 30، حيث بلغت نسبتهم 94.1%، وأقل نسبة كانت أعمارهم بالتساوي من 41 سنة إلى 50، وأقل من 30 سنة، حيث بلغت نسبتهم 0.7%.



3. **اسم الكلية:**

جدول 3: توزيع عينة الدراسة وفقاً لاسم الكلية

المتغير	الصنف	العدد	النسبة المئوية
اسم الكلية	كلية الآداب	97	63.4%
	كلية الطب	1	0.7%
	كلية التمريض	2	1.3%
	كلية الهندسة	7	4.6%
	كلية العلوم	7	4.6%
	كليات أخرى	39	25.5%
المجموع		153	100%

يوضح الجدول السابق رقم (3) أن غالبية أفراد عينة الدراسة هم من كلية الأداب حيث بلغت نسبتهم 63.4%، وأقل نسبة من عينة الدارسة هم من كلية الطب حيث بلغت نسبتهم 0.7%.

أداة جمع البيانات

تم استخدام أداة الاستبيان لدراسة " حماية البيانات الشخصية في تكنولوجيا المعلوماتية"، وقد اتبع الباحثين الخطوات الأتية لبناء الاستبانة:

1. مراجعة الدراسات السابقة ذات الصلة بموضوع الدارسة، والاستفادة منها في تطوير متغيرات الدراسة وإعداد محاور الاستبانة وصياغة فقراتها.
2. تصميم الاستبانة الأولية وعرضها على المشرف، من أجل اختبار مدى ملاءمتها لجمع البيانات اللازمة للبحث.
3. توزيع الاستبانة على عينة الدراسة، وذلك لجمع البيانات اللازمة للبحث، وقد تم تقسيم الاستبانة إلى ثلاث أقسام رئيسية، القسم الأول للتعرف على البيانات الشخصية للأفراد، والقسم الثاني (اتجاهات المستفيدين في حماية البيانات على وسائل تكنولوجيا المعلومات) ويتكون من 5 فقرات، والقسم الثالث (تغيير أراء المستفيدين نحو حماية البيانات الشخصية) ويتكون من 15 فقرة.
4. تم تصحيح أداة الدراسة حسب مقياس ليكرت الخماسي، وذلك للإجابة على فقرات القسم الثالث، والإجابات معدة حيث تكون كل فقرة لديها 5 إجابات.

جدول 4: درجات مقياس ليكرت الخماسي

الاستجابة	موافق	موافق بشدة	محايد	غير موافق	غير موافق بشدة
الدرجة	5	4	3	2	1

جدول 5: توزيع الفئات وفق التدرج المستخدم في أداة الدراسة

درجة الموافقة	قيمة المتوسط الحسابي	درجة الاستجابة
موافق تماماً	من 4.21 إلى 5	عالية جداً
موافق	من 3.41 إلى 4.20	عالية
محايد	من 2.61 إلى3.40	متوسطة
غير موافق	من 1.80 إلى 2.60	منخفضة
غير موافق إطلاقاً	من 1 إلى 1.80	منخفضة جداً

التحليل الإحصائي لأسئلة الاستبيان

تتمثل المعالجة الإحصائية لأسئلة الاستبيان فيما يلي:

- **معامل الثبات لأداة الاستبيان**

سيتم الكشف عن معامل الثبات لأداة الاستبيان، حيث يوضح مدى ثبات الاستبيان ومدى إعطائه نفس النتائج في حال تم تطبيقه مرات عديدة تحت نفس الظروف، ولقد تحقق الباحثين من ثبات الاستبيان من خلال معامل ألفا كرونباخ.

جدول 6: معامل ألف كرونباخ

عدد الفقرات	معامل ألفا كرونباخ
20	0.841

يوضح الجدول (5) معامل الثبات لفقرات الاستبيان، حيث بلغت (0.841)، وهو أعلى من معدل نابولي المتفق عليه وهو (0.70)، ويعد ذلك مؤشراً على أن أداة جمع البيانات تتسم بدرجة ثبات عالية، وبالتالي يمكن الوثوق بالنتائج التي سيتم الحصول عليها عند تطبيقها على العينة الأساسية للدراسة.

- **الإحصاءات الوصفية لأسئلة الاستبيان**

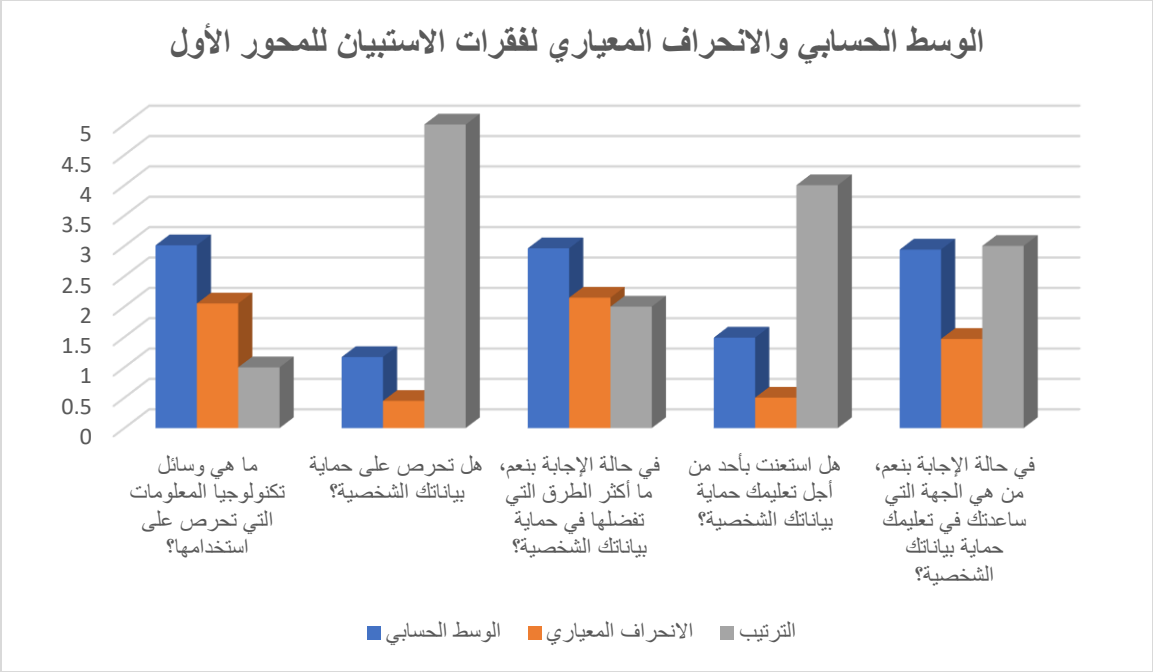
سيتم التعرف على المتوسط الحسابي والانحراف المعياري لأسئلة الاستبيان وهي كما يلي:

1. المحور الأول: اتجاهات المستفيدين في حماية البيانات على وسائل تكنولوجيا المعلومات

جدول 7: الوسط الحسابي والانحراف المعياري لفقرات الاستبيان للمحور الأول

م	العبارة	الوسط الحسابي	الانحراف المعياري	درجة الاستجابة	الترتيب
1	ما هي وسائل تكنولوجيا المعلومات التي تحرص على استخدامها؟	3.01	2.052	متوسطة	1
2	هل تحرص على حماية بياناتك الشخصية؟	1.17	0.447	منخفضة جداً	5
3	في حالة الإجابة بنعم، ما أكثر الطرق التي تفضلها في حماية بياناتك الشخصية؟	2.96	2.148	متوسطة	2
4	هل استعنت بأحد من أجل تعليمك حماية بياناتك الشخصية؟	1.49	0.501	منخفضة جداً	4
5	في حالة الإجابة بنعم، من هي الجهة التي ساعدتك في تعليمك حماية بياناتك الشخصية؟	2.94	1.468	متوسطة	3
الدرجة الكلية للمحور		**2.31**	**0.811**	متوسطة	

يوضح الجدول رقم (7) التحليل الوصفي لمعرفة عناصر المحور الأول، حيث بلغت قيمة متوسط الدرجة الكلية للبعد (2.31) وبانحراف معياري قدره (0.811)، وهذا يعني أن إجابات المبحوثين تجاه عبارات هذا البعد تسير في الاتجاه المتوسط، حيث كانت درجة استجابات العبارات متوسطة، في حين بلغت قيمة الانحرافات المعيارية ما بين (2.148) إلى (0.447)، وهذا يدل على تجانس إجابات المبحوثين.



2. المحور الثاني: تغيير أراء المستفيدين نحو حماية البيانات الشخصية

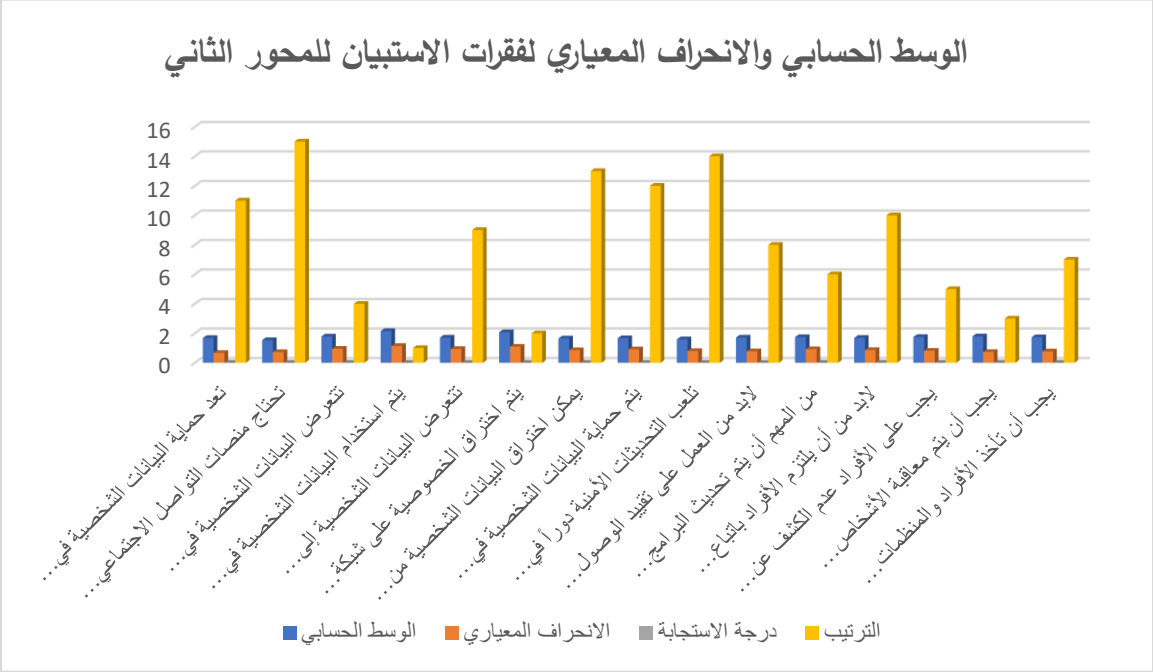
جدول 8: الوسط الحسابي والانحراف المعياري لفقرات الاستبيان للمحور الثاني

م	العبارة	الوسط الحسابي	الانحراف المعياري	درجة الاستجابة	الترتيب
1	تعد حماية البيانات الشخصية في تكنولوجيا المعلوماتية مهمة جداً.	1.68	0.665	منخفضة جداً	11
2	تحتاج منصات التواصل الاجتماعي إلى تحسين حماية البيانات الشخصية للمستخدمين.	1.54	0.726	منخفضة جداً	15
3	تتعرض البيانات الشخصية في التكنولوجيا المعلوماتية إلى انتهاكات غير قانونية.	1.78	0.948	منخفضة جداً	4
4	يتم استخدام البيانات الشخصية في التكنولوجيا المعلوماتية في بعض الأحيان بدون إذن وموافقة المستخدمين.	2.15	1.134	منخفضة	1
5	تتعرض البيانات الشخصية إلى الاختراق والسرقة على مواقع التواصل الاجتماعي.	1.71	0.932	منخفضة جداً	9

6	يتم اختراق الخصوصية على شبكة الإنترنت من قِبل مزودي خدمة الانترنت.	2.07	1.088	منخفضة	2
7	يمكن اختراق البيانات الشخصية من قِبل المواقع التي يزورها المتصفح.	1.65	0.854	منخفضة جداً	13
8	يتم حماية البيانات الشخصية في تكنولوجيا المعلوماتية من خلال تشفير البيانات وتحويلها لملفات غير قابلة للقراءة.	1.67	0.911	منخفضة جداً	12
9	تلعب التحديثات الأمنية دوراً في حماية البيانات الشخصية.	1.59	0.799	منخفضة جداً	14
10	لابد من العمل على تقييد الوصول إلى البيانات الشخصية ومنع وصول الأفراد الغير مصرح لهم بها .	1.71	0.777	منخفضة جداً	8
11	من المهم أن يتم تحديث البرامج الأمنية بشكل دوري لتأمين الأجهزة والشبكات.	1.74	0.917	منخفضة جداً	6
12	لابد من أن يلتزم الأفراد باتباع سياسة الخصوصية اللازمة لحماية البيانات الشخصية .	1.69	0.861	منخفضة جداً	10
13	يجب على الأفراد عدم الكشف عن المعلومات الشخصية لأي شخص آخر .	1.75	0.813	منخفضة جداً	5
14	يجب أن يتم معاقبة الأشخاص المنتهكين للبيانات الشخصية.	1.79	0.730	منخفضة جداً	3
15	يجب أن تأخذ الأفراد والمنظمات الإجراءات اللازمة لحماية البيانات الشخصية الخاصة بالأفراد.	1.73	0.769	منخفضة جداً	7
الدرجة الكلية للمحور		**1.75**	**0.575**	منخفضة جداً	

يوضح الجدول رقم (8) التحليل الوصفي لمعرفة عناصر المحور الثاني، حيث بلغت قيمة متوسط الدرجة الكلية للبعد (1.75) وبانحراف معياري قدره (0.575)، وهذا يعني أن إجابات المبحوثين تجاه عبارات هذا البعد تسير في الاتجاه المنخفض، حيث كانت درجة استجابات العبارات منخفضة، في

حين بلغت قيمة الانحرافات المعيارية ما بين (1.134) إلى (0.665)، وهذا يدل على تجانس إجابات المبحوثين.



الفصل الرابع: النتائج والتوصيات

النتائج

توصل البحث إلى مجموعة من النتائج ومنها ما يلي:

- بينت نتائج الدراسة بأن أفراد عينة الدراسة يستخدمون العديد من الوسائل الخاصة بتكنولوجيا المعلومات ومنها الأجهزة الذكية 39.2%، والهواتف المحمولة بنسبة 35.3%.
- أظهرت النتائج أن الأفراد يحرصون على حماية البيانات الشخصية بشكل مستمر، حيث كانت نسبة الأفراد الموافقين على هذا السؤال 85%.
- يتم استخدام العديد من الطرق في حماية البيانات الشخصية ومنها استخدام كلمات مرور قوية وتغييرها بشكل دوري وذلك بنسبة 46.4%، وعدم النقر بروابط مشبوهة بنسبة 16.3%، وتجنب مشاركة البيانات الشخصية مع مصادر غير موثوقة بنسبة 19%.
- هناك الكثير من الأفراد الذين استعانوا بمجموعة من الأفراد من أجل تعليمهم حماية البيانات الشخصية، حيث بلغت نسبتهم 51% من نسبة أفراد العينة.
- ساهم التعلم الذاتي بنسبة 45.8% والمناهج الدراسية بنسبة 7.8% والزملاء بنسبة 11.8% في تعليم أفراد عينة الدراسة حماية البيانات الشخصية.
- تبين من خلال البحث بأن حماية البيانات الشخصية في تكنولوجيا المعلومات مهم جداً، ولابد من أن يتعلم الأفراد حمايتها.
- تتطلب العديد من منصات التواصل الاجتماعي تحسين حماية البيانات الشخصية للمستخدمين، حيث أظهر غالبية أفراد العينة ذلك بنسبة 55.6%.

- تتشابه هذه الدراسة مع الدارسات السابقة، ومنها دراسة صالح (2014) في تناولها لموضوع حماية البيانات الشخصية عبر الانترنت، وأظهرت بأنه يجب أن يتم الحفاظ على خصوصية البيانات وحماية الملكية الفكرية.

التوصيات

يوصي البحث في إطار ما سبق بمجموعة من التوصيات ومنها:

- لابد من تحليل وتقييم التهديدات المحتملة للبيانات الشخصية والمعلومات الحساسة المخزنة في الأنظمة.
- وضع سياسات أمان صارمة تغطي مجموعة متنوعة من الجوانب مثل كلمات المرور القوية وسياسات التحقق من الهوية والوصول المشروط وتشفير البيانات وغيرها.
- يجب التأكد من تحديث جميع البرامج والأنظمة الخاصة بانتظام، حيث يساعد التحديث المنتظم في سد الثغرات الأمنية وتحسين قدرة النظام على حماية البيانات الشخصية.
- استخدم تقنيات التشفير لحماية البيانات الشخصية أثناء النقل والتخزين، وذلك ضمن استخدام بروتوكول HTTPS لحماية الاتصالات عبر الإنترنت واستخدام تقنيات التشفير الموثوقة لتخزين البيانات.
- يجب توعية الموظفين والمستخدمين بشأن أهمية حماية البيانات الشخصية والممارسات الأمنية المناسبة، عن طريق تقديم تدريبات وورش عمل وإرشادات سهلة الفهم، يمكن تعزيز الوعي بأمان المعلومات وتقليل المخاطر.

الخاتمة

تعتبر حماية البيانات الشخصية مطلباً هاماً في كل الأمور، وخاصة في إطار التطورات التكنولوجية في الوقت الحاضر، حيث أن التكنولوجيا لعبت دور في اختراق الأجهزة والحسابات الشخصية واستغلال البيانات الشخصية من أجل أسباب مختلفة ولقد تم التطرق إلى هذا الموضوع من أجل حل هذه المشكلة وتقديم بعض النصائح اللازمة لحماية البيانات الشخصية، ولقد تم اختيار المنهج الوصفي التحليلي لدراسة مشكلة البحث، وذلك كونه يعتبر من أكثر المناهج التي تساهم في وصف المشكلة وصفاً دقيقاً وتساعد في جمع المعلومات اللازمة وإيجاد الوسائل المختلفة لتفسيرها، كما أنه تم تصميم أداة الاستبيان من أجل جمع المعلومات اللازمة عن موضوع الدراسة.

وقد استنتجنا من خلال هذه الدراسة التي قمنا بها في جامعة طيبة بأن غالبية أفراد العينة يحرصون على حماية البيانات الشخصية الخاصة بهم، ويستخدمون العديد من الأدوات والوسائل للمحافظة عليها ومنها تشفير البيانات، واستخدام خدمات VPN الافتراضية، وكذلك فإنه قد تبين بأن العديد من أفراد جامعة طيبة يستخدمون الدورات التدريبية والمناهج الدراسية لتعلم حماية البيانات.

المراجع

1. أحمد، هندي. (2017). قانون حماية البيانات الشخصية في مواقع التواصل الاجتماعي لمؤسسات المكتبات والمعلومات. المؤتمر الثامن والعشرون: شبكات التواصل الاجتماعي وتأثيراتها في مؤسسات المعلومات في الوطن العربي. القاهرة. ص1-25.
2. أعزان، أمين. (2013). حماية البيانات الشخصية للمستهلك الإلكتروني. مجلة الاقتصاد والمستهلك: ع6. ص20.
3. بطيحي، نسمة، (2019). الجرائم المتعلقة بانتهاك الأحكام الإجرائية المقررة لحماية الحق في الخصوصية الرقمية في التشريع الجزائري، كتاب أعمال المؤتمر الدولي حول الخصوصية في مجتمع المعلوماتية، مركز جيل البحث العلمي، لبنان، طرابلس.
4. التهامي، سامح. (2011). الحماية القانونية للبيانات الشخصية: دراسة القانون الفرنسي – القسم الأولى. مجلة الحقوق: مج35(3). ص375-434.
5. خلايفة، هدى، (2019). الإطار القانوني الدولي والداخلي لحماية الخصوصية على الانترنت، التشريع الجزائري نموذجاً، كتاب أعما المؤتمر الدولي المحكم حول الخصوصية في مجتمع المعلوماتية، مركز جيل البحث العلمي، لبنان، طرابلس.
6. داود، إبراهيم. (2017). الحماية القانونية للبيانات الشخصية من منظور الحق في الخصوصية. مجلة كلية الحقوق للبحوث القانونية والاقتصادية: ع1. ص315-456.
7. الصيادي، آمنة، (2019). البيانات الشخصية، ما مدى أهمية حمايتها وهل من تشريع؟ منظمة أكسس ناو. الرابط الالكتروني: https://cutt.us/BA6kJ. تاريخ الاسترداد: 2023/4/16.

8. الضناوي، زينب، (2019). الحامية القانونية للخصوصية على الانترنت فيظل الجهود الدولية والداخلية، كتاب أعمال المؤتمر الدولي المحكم حول الخصوصية في مجتمع المعلوماتية، مركز جيل البحث العلمي، لبنان، طرابلس.

9. عزي، عبير، (2015). تأثيرات استخدام المعلنين لتقنيات التتبع الجغرافي للمستهلكين عبر الهواتف الذكية. المجلة العلمية لبحوث العلاقات العامة والاعلان.

10. عبد ربة، محمد. (2018). حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي. دراسة مقارنة. مجلة كلية الشريعة والقانون بطنطا: ع44. ص1926-2057.

11. العكيلي، علي. (2022). الحماية الدستورية للبيانات الشخصية. المجلة الأكاديمية للبحوث القانونية والسياسية: مج6(1). ص1-14.

12. العجمي، أحمد. (2023). الحق في خصوصية البيانات الشخصية وضمانات حمايتها في عصر التحول الرقمي: دراسة تحليلية في النظام السعودي. معهد الإدارة العامة: ع3. ص481-510.

13. علي، محمد. (2021). النظام القانوني لحماية البيانات الشخصية المعالجة إلكترونيا: دراسة تحليلية مقارنة في ضوء اللائحة الأوربية وبعض التشريعات ذات العلاقة. مجلة العلوم القانونية: مج7(14). ص73-118.

14. غالب، عبد القادر. (2019). قانون حماية البيانات الشخصية. مجلة الاقتصاد الإسلامي العالمية: ع87. ص50-54.

15. فقيه، جيهان. (2017). حماية البيانات الشخصية في الإعلام الرقمي. مجلة العلوم الإنسانية: ع7. ص1112-9255.

16. كمال، أحمد. (2009). حماية البيانات الشخصية على شبكة الإنترنت. المجلة الجنائية القومية: مج52(2). ص63-100.

17.اللمكية، ألاء وآخرون. (2015). حماية البيانات الشخصية لمستخدمي شبكات التواصل الاجتماعي. رسالة ماجستير. كلية الحقوق. جامعة السلطان قابوس. عمان.

18.الموسوي، منى، وفضل الله، جان، (2013). الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها. مجلة كلية بغداد للعلوم الاقتصادية الجامعة، العدد الخاص بمؤتمر الكلية.

19.مشعل، محمد. (2017). الحق في محو البيانات الشخصية: دراسة تحليلية في ضوء لائحة حماية البيانات بالاتحاد الأوروبي GDPR وأحكام المحاكم الأوروبية. مجلة الدراسات القانونية والاقتصادية: مج3(2). ص1–293.

20.يس، إيمان. (2022). الخصوصية وحماية البيانات الشخصية بالمكتبات: مراجعة علمية. المجلة الدولية لعلوم المكتبات والمعلومات: مج9(2). ص477–493.

الملاحق

بسم الله الرحمن الرحيم

الأخ/ الأخت: ..... حفظه الله ورعاه

السلام عليكم ورحمة الله وبركاته

الموضوع: المشاركة في تعبئة استبانة الدراسة بعنوان:

حماية البيانات الشخصية في تكنولوجيا المعلوماتية

يطيب لنا أنْ نضع بين أيديكم هذه الاستبانة التي تم إعدادها من أجل الحصول على البيانات المتعلقة بالدراسة وذلك استكمالاً لمتطلبات الحصول على درجة البكالوريوس في تخصص علم المعلومات في جامعة طيبة، وذلك بإشراف الدكتور/ **أسامة حامد**، بعنوان: **حماية البيانات الشخصية في وسائل تكنولوجيا المعلوماتية**، لذا نرجو التكرم من سيادتكم بتخصيص جزء من وقتكم الثمين من أجل تعبئة الاستبانة وذلك بوضع علامة أمام الإجابة التي تعبر عن وجهة نظرك، مع مراعاة الدقة والموضوعية في الإجابة عن الأسئلة المطروحة، حيثُ سيكون لإجابتكم عظيم الأثر والفائدة من أجل الوصول لنتائج تتسم بالدقة، على أنْ يتم التعامل مع هذه المعلومات والبيانات الواردة في الاستبانة بسرية تامة ولن يتم استخدامها إلا لأغراض البحث العلمي فقط .

شاكرين لكم تعاونكم وتقبلوا منا فائق الاحترام والتقدير.

بسم الله الرحمن الرحيم

الموضوع: المشاركة في تعبئة استبانة الدراسة بعنوان:

حماية البيانات الشخصية على وسائل تكنولوجيا المعلومات

الاسم: "اختياري" _____

القسم الأول: البيانات الشخصية

يرجي وضع علامة أمام الإجابة الملائمة:

1. الجنس: ذكر ( ) أنثى ( )

2. العمر:

اقل من 20 سنة الى30( )

من 31 إلى41 سنة ( )

من سنة 41 الى 49 سنة( )

من50 فما فوق( )

3. اسم الكلية:

كلية الآداب

كلية الطب

كلية التمريض

كلية الهندسة

كلية العلوم

كليات اخري

القسم الثاني: اتجاهات المستفيدين في حماية البيانات على وسائل تكنولوجيا المعلومات

1- ما هي وسائل تكنولوجيا المعلومات التي تحرص على استخدامها؟

- الحواسيب
- الأجهزة الذكية
- الهواتف المحمولة
- برامج التصميم الجرافيكي
- برامج المعالجة النصية
- برامج الحماية والأمان
- تقنية الواي فاي والبلوتوث
- التطبيقات
- الخوادم
- الشبكات والإنترنت
- الاتصالات
- قواعد البيانات
- البرمجيات
- أخرى

2- هل تحرص على حماية بياناتك الشخصية؟

نعم() الى حد ما( ) لا( )

في حالة الإجابة بنعم:

3- ما أكثر الطرق التي تفضلها في حماية البيانات الشخصية؟

- استخدام كلمات مرور قوية وتغييرها بشكل دوري
- استخدام تقنية التشفير
- تحديث البرامج والأنظمة بشكل دوري
- عدم النقر على روابط مشبوهة
- تجنب مشاركة البيانات الشخصية مع مصادر غير موثوقة
- استخدام برامج مكافحة الفيروسات والبرامج الضارة
- عدم تخزين البيانات الشخصية بشكل غير آمن
- أخرى

4- هل استعنت بأحد من أجل تعليمك حماية البيانات الشخصية؟

نعم ( ) لا ( )

في حالى الإجابة بنعم

5- من هي الجهة التي ساعدتك في تعليمك حماية بياناتك الشخصية؟

-زملاءك

- التعلم الذاتي
- المناهج الدراسية

-الدورات التدريبية

- أخرى

القسم الثالث: أراء المستفيدين نحو حماية البيانات الشخصية

الرجاء الإجابة عن الأسئلة التالية بوضع إشارة على الإجابة المناسبة من وجهة نظرك.

م	العبارة	موافق	موافق بشدة	محايد	غير موافق	غير موافق بشدة
1	تعد حماية البيانات الشخصية في تكنولوجيا المعلوماتية مهمة جداً.					
2	تحتاج منصات التواصل الاجتماعي إلى تحسين حماية البيانات الشخصية للمستخدمين.					
3	تتعرض البيانات الشخصية في التكنولوجيا المعلوماتية إلى انتهاكات غير قانونية.					
4	يتم استخدام البيانات الشخصية في التكنولوجيا المعلوماتية في بعض الأحيان بدون إذن وموافقة المستخدمين.					
5	تتعرض البيانات الشخصية إلى الاختراق والسرقة على مواقع التواصل الاجتماعي.					
6	يتم اختراق الخصوصية على شبكة الإنترنت من قِبل مزودي خدمة الانترنت.					
7	يمكن اختراق البيانات الشخصية من قِبل المواقع التي يزورها المتصفح.					
8	يتم حماية البيانات الشخصية في تكنولوجيا المعلوماتية من خلال تشفير البيانات وتحويلها لملفات غير قابلة للقراءة.					
9	تلعب التحديثات الأمنية دوراً في حماية البيانات الشخصية.					

10	لابد من العمل على تقييد الوصول إلى البيانات الشخصية ومنع وصول الأفراد الغير مصرح لهم بها.					
11	من المهم أن يتم تحديث البرامج الأمنية بشكل دوري لتأمين الأجهزة والشبكات.					
12	لابد من أن يلتزم الأفراد باتباع سياسة الخصوصية اللازمة لحماية البيانات الشخصية.					
13	يجب على الأفراد عدم الكشف عن المعلومات الشخصية لأي شخص آخر.					
14	يجب أن يتم معاقبة الأشخاص المنتهكين للبيانات الشخصية.					
15	يجب أن تأخذ الأفراد والمنظمات الإجراءات اللازمة لحماية البيانات الشخصية الخاصة بالأفراد.					

نشكر لكم حسن تعاونكم معنا...