إدارة الخصوصية المعلوماتية لمستخدمي تطبيقات الصحة المتنقلة: دراسة تحليلية وميدانية

إعداد
د. زينب علي بكري علي
مدرس بقسم المكتبات والمعلومات
قسم المكتبات وتكنولوجيا المعلومات
كلية الآداب- جامعة جنوب الوادي(قنا)
zeinabbakry@art.svu.edu.eg

الملخص

تنامي في السنوات الأخيرة بشكل مطرد سوق تطبيقات الصحة المتنقلة mobile Health apps المستخدمة في الهواتف الذكية، والتي على الرغم من فوائدها إلا أنها تطرح عددا من المشكلات التي تتعلق بالخصوصية بسبب البيانات الشخصية والحساسة التي يمكنها الوصول إليها، لذا سعت هذه الدراسة إلى دراسة وتحليل سياسات الخصوصية لتطبيقات الصحة المتنقلة mHealth apps المتاحة على النسخة المصرية من متجر جوجل بلاي، للكشف عن ممارساتها ونوع وطبيعة البيانات التي تجمعها من المستخدمين والتحقق من التزامها بلوائح وقوانين الخصوصية، وكذلك التعرف على اتجاهات مستخدمي تلك التطبيقات نحو الخصوصية وممارساتهم في إدارة وحماية خصوصيتهم. وقد استخدمت الباحثة المنهج الوصفي التحليلي، معتمدة في ذلك على أداتين للدراسة وهما قائمة المراجعة لتحليل مضمون سياسات الخصوصية للتطبيقات عينة الدراسة والبالغ عددها (١٥٣) تطبيق، والأخرى استبانة الكترونية لكشف ممارسات مستخدمي تلك التطبيقات لإدارة خصوصيتهم، وخلصت الدراسة إلى عدد من النتائج من أهمها: أن مستوى امتثال مقدمو الخدمة بتطبيقات الصحة المتنقلة عينة الدراسة للوائح وقوانين الخصوصية ومدى التزامهم بالكشف عن ممارساتهم حيال خصوصية المستخدمين كان ضعيفا بمتوسط حسابي بلغ (٠,٣٢). تم تصنيف نسبة (٣٩,٩٪) من التطبيقات على أنها ذات مخاطر خصوصية مرتفعة، بينما صُنفت نسبة (٣٤,٦٪) بأنها ذات مخاطر خصوصية مرتفعة جدا، هناك نسبة (٤٦,٢٪) من أفراد العينة يستخدمون بالفعل تطبيقات الصحة المتنقلة على هواتفهم الذكية، كما أفادت نسبة (٤٦,٢٪) من مستخدمي تلك التطبيقات بأنهم لم يقرأوا أبدا سياسات الخصوصية لتطبيقات الصحة المتنقلة قبل تثبيتها على هواتفهم المحمولة. وأوصت الدراسة بضرورة عمل حملات توعية لتثقيف المواطنين بشأن حقوقهم وواجباتهم تجاه خصوصيتهم الرقمية وطرق مواجهة انتهاكات الخصوصية، وتوعيتهم بوجود قانون لحماية البيانات الشخصية في مصر، لأن الرفع من وعي مستخدمي التطبيقات بالخصوصية من شأنه دفع مطوري التطبيقات على التعامل مع بيانات المستخدم بشكل أكثر مسؤولية.

الكلمات المفتاحية:

سياسات الخصوصية؛ الخصوصية المعلوماتية؛ حماية الخصوصية؛ تطبيقات الصحة المتنقلة؛ الهواتف الذكية.

تمهيد:

لا نزاع اليوم في أن الخصوصية تُعد من الحقوق الدستورية الأساسية الملازمة للشخص الطبيعي بصفته الإنسانية كأصل عام، فهي تُعد أساس بنيان كل مجتمع سليم**(مصطفى، ٢٠١٦)**، وتعتبر الخصوصية واحدة من الأشياء المرتبطة بالأمان النفسي والشعور بالقدرة على التحكم في محيط الفرد. ومع الاعتماد المتزايد على التكنولوجيا الرقمية وتطورها المستمر، تغير مفهوم الخصوصية بمرور الوقت سواء بالنسبة لمستخدمي التكنولوجيا، أو حتى بالنسبة لمطوريها. فالتطورات الحديثة في تكنولوجيا الاتصال

تاريخ استلام البحث : ٢٧ أكتوبر ٢٠٢٣ ، تاريخ القبول : ١٣ ديسمبر ٢٠٢٣

منحت الفرصة لطرف ثالث بخلاف طرفي الاتصال بالتحكم في ملفات المستخدمين ومراقبتها. وبناءً عليه تطور مفهوم الخصوصية من الحق في البقاء منفردا "The right to be let alone" إلى الحق في التحكم في المعلومات الشخصية **(Chen, 2018)**.

حيث يشهد عصرنا الحالي جدلا واسعا حول خصوصية الأفراد المستخدمين للإنترنت وحمايتهم من خطر التهديد والابتزاز والأذى بكافة أشكاله، فما صرح به أرفيند نارايانان Arvind Narayanan أستاذ علوم الكمبيوتر في جامعة برينستون " أنه بمجرد أن تحصل إحدى الجهات على بياناتنا، فإنها تعمل على تخزينها إلى الأبد، فهناك شركات تتخصص في جمع البيانات عنا من مصادر مختلفة لإنشاء ملفات افتراضية وإنشاء تطبيقات لاستخراج البيانات للتأثير علينا بطرق مختلفة **(عبد الله، ٢٠١٩)**، وما صرحت به أيضا مارغو سيلتزر Margo Seltzer مؤخرا في المنتدى الاقتصادي العالمي من تصريحا يوحي بوفاة الخصوصية حيث قالت" لم يعد من الممكن العودة إلى الخصوصية التي كنا نعرفها في الماضي...كما ماتت الطريقة التي كنا نفكر فيها بالخصوصية"**(Yerukhimovich, et al, 2016)** وهي جميعها تصريحات تدعو حقا لإثارة القلق وضرورة البحث والتقصي في حقيقة هذه المشكلة.

ومع ما أحدثه انتشار الهواتف الذكية والتي أصبحت جزءا لا يتجزأ من الحياة اليومية من ثورة في حياة الإنسان، حيث يسعى كل قطاع من قطاعات المجتمع إلى الاستفادة منها **(Lane, et al., 2020)**. نجد أن قطاع الصحة يشارك بقوة في هذه الثورة اليوم، فظهرت العديد من الأجهزة والتطبيقات المحمولة في المجالات الصحية والطبية مثل ساعات المعصم والأساور والأجهزة الأخرى المحمولة أو القابلة للارتداء وغيرها من التطبيقات والتي تؤدي العديد من الوظائف بدءا من إدارة الحالات الصحية وفحص الأعراض ومراقبة درجة الحرارة وضغط الدم والسكر ومستوى السعرات الحرارية واللياقة البدنية ومستويات الكوليسترول واقتراح أنظمة غذائية صحية ومتابعة صحة المرأة والحوامل، وما إلى ذلك **(Apuru & Andembubtob & Audu Dodo, 2017)**.

وعلى الرغم مما ذكره **Huuskonen, et al. (2015)** من فوائد لتطبيقات الصحة المتنقلة mobile Health apps من تحسين الظروف المعيشية للمواطنين وزيادة الوصول إلى المعلومات الصحية؛ والذي بدوره يساعد المجتمع على تقليل الإنفاق غير الضروري على الرعاية الصحية ويساعد أيضًا في ضمان صحة المواطنين. إلا أنها تطرح الكثير من المشكلات منها ما يتعلق بخطر التشخيص أو الاستخدام الخاطئ، ومنها ما يتعلق بخصوصية البيانات بسبب المعلومات الشخصية والحساسة التي تجمعها تلك التطبيقات عن المستخدم فضلا عن مشاركة البيانات مع أطراف أخرى وعدم تطبيق معايير الخصوصية مما يجعلها تشكل العديد من المخاطر الأمنية الكبيرة على خصوصية المستخدمين.

أولا: الإطار المنهجي للدراسة:

١/١ مشكلة الدراسة :

تنامي في السنوات الأخيرة سوق تطبيقات الصحة المتنقلة mHealth المستخدمة في الهواتف الذكية بشكل مطرد، ففي عام ٢٠١٧ تم حصر ٣٢٥٠٠٠ تطبيقا أتيحت في متاجر التطبيقات الرئيسية على مستوى العالم، وقد قدر هذا بزيادة قاربت نسبة ٣٢٪ على عام ٢٠١٦**(مؤمنة، ٢٠٢٢)**.

وقد لاحظت الباحثة الاستخدام المتزايد لتطبيقات الصحة المتنقلة mHealth apps من قبل الكثير من الأفراد المحيطين بها سواء كانوا مرضى أم مجرد راغبين في تحسين وضعهم الصحي، دون أن يولي هؤلاء اهتمامًا كافيًا بما يتم جمعه من بيانات شخصية وحساسة عند تنزيل وتثبيت هذه التطبيقات على هواتفهم الذكية، أو بما يتعين عليهم منحه من أذونات معينة لتلك لتطبيقات للوصول إلى بيانات معينة على

أجهزتهم قبل أن يتمكنوا من تثبيتها أو استخدامها، حيث تتطلب تطبيقات mHealth العديد من البيانات الشخصية والحساسة لتقديم خدماتها، وهو ما أثار انتباه وفضول الباحثة وجعلها تتساءل:

- هل يلتزم مطورو تطبيقات mHealth بالإفصاح والكشف عن ممارساتهم نحو خصوصية بيانات المستخدمين وإبلاغهم بكيفية جمع معلوماتهم الشخصية ومعالجتها وحفظها؟
- هل مستخدمي تطبيقات mHealth على دراية بمخاطر الخصوصية التي قد تنشأ حيال جمع واستخدام ومشاركة بياناتهم الشخصية؟ وهل بإمكانهم إدارة خصوصيتهم داخل تلك التطبيقات؟
- ومن هنا جاءت فكرة الدراسة حيث أن الإفصاح عن ممارسات الخصوصية يُعد مطلبا قانونيا تحدده لوائح وقوانين الخصوصية، كما أن البيانات الصحية هي بيانات حساسة بحكم طبيعتها وبموجب القانون أيضا.

ومن ثم يمكن صياغة مشكلة الدراسة على النحو التالي " دراسة وتحليل سياسات الخصوصية لتطبيقات الصحة المتنقلة mHealth apps المتاحة على النسخة المصرية من متجر جوجل بلاي للكشف عن ممارساتها ونوع وطبيعة البيانات التي تجمعها من المستخدمين والتحقق من التزامها بلوائح وقوانين الخصوصية، والتعرف على اتجاهات مستخدمي تلك التطبيقات نحو الخصوصية وممارساتهم في إدارة وحماية خصوصيتهم".

٢/١ أهداف الراسة:

تسعى الدراسة إلى تحقيق هدفين رئيسيين، ويندرج تحت كل منهما عدد من الأهداف الفرعية:

- **الهدف الأول:** تحليل سياسات الخصوصية لعينة من تطبيقات mHealth المتاحة على النسخة المصرية من متجر جوجل بلاي للتأكد من توافقها مع قوانين الخصوصية، ومدى التزامها بالممارسات المسؤولة لحماية البيانات الشخصية لمستخدميها، ويندرج تحت هذا الهدف عدة أهداف فرعية وهي:
  - التعرف على الموضوعات والقضايا التي تناولتها سياسات الخصوصية لتلك التطبيقات.
  - رصد واقع ممارسات الخصوصية التي يتبعها مطورو تطبيقات الصحة المتنقلة.
  - رصد مدى التزام مطورو التطبيقات بالكشف عن ممارسات الخصوصية الخاصة بجمع ومشاركة ونقل البيانات الشخصية والحساسة للمستخدمين.
  - استكشاف مدى الحماية التي توفرها تلك التطبيقات لمستخدميها.
  - حصر أنواع البيانات الشخصية التي تجمعها تلك التطبيقات من المستخدمين.
  - التعرف على أنواع الأذونات التي تطلبها تلك التطبيقات.
- **الهدف الثاني:** الكشف عن واقع الاستخدام لتلك التطبيقات ومدى وعي مستخدميها بآليات حماية الخصوصية، ويندرج تحت هذا الهدف عدة أهداف فرعية:
  - الكشف عن واقع ومعدل استخدام عينة الدراسة لتطبيقات الصحة المتنقلة.
  - التعرف على اتجاهات مستخدمي تطبيقات الصحة المتنقلة نحو الخصوصية.
  - رصد الممارسات التي يقوم بها مستخدمي تطبيقات الصحة المتنقلة لإدارة وحماية خصوصيتهم.

٣/١ تساؤلات الدراسة:

تسعى الدراسة إلى الإجابة على التساؤلات التالية:

أولا: تساؤلات الدراسة التحليلية لسياسات الخصوصية لتطبيقات الصحة المتنقلة عينة الدراسة:

١) ما مدى التزام تلك التطبيقات بحماية الحق في الخصوصية لمستخدميها؟
٢) ما مدى وضوح سياسات الخصوصية لتطبيقات الصحة المتنقلة عينة الدراسة؟
٣) ما أهم الموضوعات والقضايا التي تناولتها سياسات الخصوصية لتلك التطبيقات؟
٤) ما مستوى التزام مطوري تطبيقات الصحة المتنقلة بالكشف عن ممارساتهم نحو خصوصية بيانات المستخدمين؟
٥) ما طبيعة البيانات التي تجمعها تلك التطبيقات من المستخدمين؟
٦) ما أنواع الأذونات التي تطلبها تلك التطبيقات؟
٧) هل تتشارك تلك التطبيقات البيانات التي تجمعها مع أطراف أخرى؟ وهل تحرص على ذكر هذه الأطراف صراحة؟
٨) كيف يحافظ مطورو تلك التطبيقات على خصوصية وأمان بيانات المستخدمين الشخصية والحساسة؟

ثانيا: تساؤلات الدراسة الميدانية:

٩) ما معدل استخدام أفراد العينة لتطبيقات الصحة المتنقلة ؟
١٠) ما اتجاهات مستخدمو تطبيقات الصحة المتنقلة نحو الخصوصية؟
١١) ما الممارسات التي يقوم بها مستخدمي تطبيقات الصحة المتنقلة لإدارة وحماية خصوصيتهم؟

٤/١ أهمية الدراسة:

تستمد الدراسة الحالية أهميتها من الآتي:

- إلقاء الضوء على مفهوم الخصوصية في بيئة الهواتف الذكية باعتباره من المجالات البحثية الحديثة وخاصة في ظل تنامي الاهتمام العالمي بمجال حماية البيانات الشخصية.
- رفع وعي مطوري تطبيقات الهواتف الذكية بقوانين ولوائح الخصوصية، لضمان التزامهم بالسياسات والمعايير لتوفير الحماية لمستخدميها.
- تعد هذه الدراسة من الدراسات الاستكشافية حول تقصي حالة الخصوصية لمستخدمي تطبيقات الصحة المتنقلة mHealth والخروج بتصور عام عن واقع سلوك مستخدميها فيما يتعلق بخصوصية بياناتهم الشخصية والحساسة لعل ذلك يساعد في توعية الأفراد بحقهم في حماية حياتهم الخاصة من أي انتهاك أو تعدي عليها.
- ترى الباحثة أن زيادة وعي مستخدمي تطبيقات الهواتف الذكية بلوائح الخصوصية وقوانينها قد يضمن التزام مطورو التطبيقات بسياسات الخصوصية التي يضعونها في تطبيقاتهم.

- قد يستفيد مشرعو القوانين من الدراسة في فهم قضايا وجوانب الخصوصية بشكل أكبر مما يساعدهم في وضع الإطار التشريعي والقانوني المناسب للتصدي للقضايا المرتبطة بأمن وخصوصية الهواتف الذكية وتطبيقاتها، مما يعزز من ثقة الأفراد في التعامل معها.

٥/١ منهج الدراسة:

اعتمدت الباحثة في دراستها على المنهج الوصفي التحليلي، بوصفه أنسب المناهج لرصد واقع ممارسات الخصوصية التي يتبعها مطورو تطبيقات الصحة المتنقلة mHealth apps وذلك عن طريق تحليل مضمون سياسات الخصوصية لتلك التطبيقات، بالإضافة إلى جمع البيانات والحقائق عن الظاهرة كما هي في الواقع وتحليلها وتفسيرها للكشف عن واقع الاستخدام لتطبيقات الصحة المتنقلة واتجاهات وممارسات مستخدميها نحو الخصوصية.

٦/١ مجتمع وعينة الدراسة:

١) **بالنسبة لتطبيقات الصحة المتنقلة:** يتمثل مجتمع الدراسة في جميع تطبيقات الصحة المتنقلة mHealth apps المتاحة على متجر جوجل بلاي (فئة الطب، وفئة الصحة واللياقة البدنية)، والبالغ عددها وفقا لإحصائيات يناير ٢٠٢٣[١] في فئة الصحة واللياقة البدنية (٩٥٢٤٤) و (٤١١٠٨) في فئة الطب، وبالنسبة لعينة الدراسة فتمثلت في تطبيقات الصحة المتنقلة المجانية فقط والمتاحة على قائمة الأكثر رواجا Top Charts على النسخة المصرية من متجر جوجل بلاي والبالغ عددهم ٣٩١ تطبيق(١٩٥ في فئة الصحة واللياقة البدنية و ١٩٦ في فئة الطب) وذلك وفقا لحصر قامت به الباحثة بتاريخ ٢٠٢٣/٤/٩، وقد اختارت الباحثة فئة التطبيقات المجانية فقط لأنها الأكثر شيوعا وذلك من واقع عدد عمليات التحميل، مما يجعلها قد تهدد خصوصية آلاف بل ملايين المستخدمين، ولصعوبة تحليل سياسة الخصوصية لهذا العدد من التطبيقات، فقد اختارت الباحثة عينة من التطبيقات تنطبق عليها الشروط التالية:

- أن لا يقل عدد عمليات التنزيل للتطبيق عن ١٠٠ ألف.
- أن يحصل التطبيق على درجة تقييم لا تقل عن ٤.
- ألا يكون تطبيق موجه لمقدمي خدمات الرعاية الصحية والمهنيين لإدارة عملهم.
- ألا يكون مرجعا تعليميا لطلاب الطب والتمريض.
- ألا يكون تطبيقا لطلب الأدوية.
- ألا يكون تطبيقا لموسيقى الاسترخاء أو تعقب النوم أو تذكير شرب الماء لما قد يكون لها من تأثير أقل على الخصوصية.

وقد انطبقت تلك الشروط على ١٥٤ تطبيق (١٣١ في فئة الصحة واللياقة البدنية و٢٣ في فئة الطب). ولكن تم تحليل سياسات الخصوصية لـ (١٥٣) تطبيق حيث تم استبعاد تطبيق واحد فقط لم يتضمن سياسة خصوصية، وتُرجع الباحثة التزام غالبية مقدمو الخدمة لتطبيقات الصحة المتنقلة بتوفير سياسة خصوصية للتطبيق إلى القرار الذي اتخذه متجر جوجل بلاي في عام ٢٠١٨ بفرض توفير سياسة خصوصية لأي تطبيق حتى يتم إدراجه في المتجر

٢) **بالنسبة للدراسة الميدانية:** فيتمثل مجتمع الدراسة في جميع مستخدمي تطبيقات الصحة المتنقلة في المجتمع المصري، حيث تم طرح الاستبانة بشكل رقمي لفترة تقارب من شهرين من ٦/٧ إلى

٢٠٢٣/٨/١، حيث أجابت عليه عينة قدرت ب (٢١٠) مفردة شملت عدة شرائح عمرية واجتماعية وتعليمية.

٧/١ أدوات الدراسة:

استخدمت الباحثة أداتين لجمع البيانات وهما :

أ. **قائمة المراجعة:** استخدمت الباحثة قائمة مراجعة أُعدت خصيصا لتحليل محتوى ومضمون سياسات الخصوصية للتطبيقات عينة الدراسة، والتي تم بنائها في ضوء اللائحة العامة لحماية البيانات (GDPR) ومواد القانون المصري رقم ١٥١ لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية، ويوضح الجدول رقم (١) محاور قائمة المراجعة والتي تكونت من ٣٥ بند موزعة على ٨ محاور رئيسية، بالإضافة إلى حصر البيانات التي تجمعها تطبيقات الصحة المتنقلة عينة الدراسة، والأذونات التي تطلبها.

جدول رقم (١): محاور وبنود قائمة المراجعة

المحاور	عدد البنود	النسبة المئوية
قواعد وممارسات عامة	8	22.9%
جمع البيانات	5	14.3%
أغراض جمع وتحليل البيانات	4	11.4%
مشاركة البيانات مع أطراف ثالثة	8	22.9%
تأمين البيانات	3	8.6%
حق المستخدم وسيطرته على بياناته	3	8.6%
الإبلاغ عن تحديث أو تعديل سياسة الخصوصية	2	5.7%
الإبلاغ عن تسريب البيانات	2	5.7%
المجموع	35	100%

ب. **استبانة الكترونية**: طبقت استمارة استبانة الكترونية مكونة من (١٧) سؤالا، موزعة على ثلاث محاور(البيانات الديموجرافية، واقع الاستخدام، اتجاهات وممارسات الخصوصية) تم توزيعها بالاستعانة ب Google Forms، عن طريق نشرها عبر مواقع وتطبيقات مختلفة مثل (فيس بوك، واتس آب)، في محاولة للوصول لأكبر عدد من مستخدمي تطبيقات الصحة المتنقلة mHealth apps بمصر.

١/٧/١ الصدق الظاهري لأدوات الدراسة:

قامت الباحثة بعرض قائمة المراجعة والاستبانة على ثلاثة من المحكمين المتخصصين في مجال علم المكتبات والمعلومات والقانون[٢]، والذين تفضلوا بإدخال بعض التعديلات والتي التزمت الباحثة بها، وفي ضوء آرائهم تم إعداد أدوات الدراسة في صورتها النهائية، وقد شملت التعديلات التي أدخلت تعديل صياغة بعض العبارات والأسئلة، وتعديل معيار التقييم في السؤال السابع عشر في الاستبانة من اختيار أكثر من بديل للإجابة إلى مقياس ثلاثي.

٢/٧/١ ثبات الاستبانة:

لقياس مدي ثبات الاستبانة تم حساب معامل ألفا كرونباخ لجميع فقراتها، حيث أجرت الباحثة دراسة قبلية على عينة قوامها (١٤) مفردة، واتضح من النتائج أن معامل الثبات بلغ (٠,٨٥٣)، مما يدل علي أن الاستبانة تتمتع بدرجة جيدة من الثبات يمكن الاعتماد عليها في التطبيق الميداني.

٨/١ حدود الدراسة:

- **الحدود الموضوعية**: تتمثل في دراسة وتحليل سياسات الخصوصية لعينة من تطبيقات الصحة المتنقلة mHealth للكشف عن ممارسات الخصوصية لتلك التطبيقات، والكشف عن واقع الاستخدام لتلك التطبيقات ومدى وعي مستخدميها بآليات حماية الخصوصية .
- **الحدود النوعية**: تنحصر في تطبيقات الصحة المتنقلة المجانية والمدرجة في فئتي الطب والصحة واللياقة البدنية على النسخة المصرية من متجر جوجل بلاي.
- **الحدود الزمنية**: امتدت فترة الدراسة التحليلية لسياسات الخصوصية لمدة شهرين(مايو/ يونيه ٢٠٢٣)، بينما امتدت فترة الدراسة الميدانية من(٧ يونيه حتى ١ أغسطس ٢٠٢٣).
- **الحدود المكانية**: اقتصرت على تطبيقات الصحة المتنقلة المتاحة على النسخة المصرية من متجر جوجل بلاي، ومستخدميها في مصر.

٩/١ مصطلحات الدراسة:

- **الخصوصية Privacy**: "هي حق الفرد أو المجموعة في الحفاظ على المعلومات المرتبطة بحياتهم الشخصية والمهنية من الإفصاح عنها، وخاصة للمؤسسات الحكومية والتجارية وعدم المراقبة باستثناء ما هو مصرح به بموجب أحكام القانون" **(Reitz, 2014).**

وتعرف الباحثة الخصوصية المعلوماتية إجرائيا بأنها" حق مستخدم تطبيقات الصحة المتنقلة في الحفاظ على سرية بياناته الشخصية والحساسة المتعلقة بهويته أو سلوكه أثناء استخدام التطبيق وعدم تداولها دون إذن مسبق منه بحيث يُحدد بنفسه متى، وكيف يمكن لمعلوماته الشخصية والحساسة أن تصل لمطوري تلك التطبيقات وإلى أي مدى يمكن مشاركتها مع أطراف أخرى".

- **سياسة الخصوصية Privacy policy :** وفقا للدراسة يمكن تعريفها **إجرائيا** على أنها" وثيقة إلكترونية ينشئها مطورو تطبيقات الصحة المتنقلة ترسم الإجراءات وتكشف الممارسات التي يتم بها جمع وتخزين ومشاركة بيانات المستخدم الشخصية فهي بمثابة اتفاقية بين المستخدمين ومطوري التطبيقات".
- **الصحة المتنقلة (mHealth) mobile Health:** تعرفها منظمة الصحة العالمية على أنها" الممارسات الطبية وممارسات الصحة العامة المدعومة بأجهزة محمولة مثل الهواتف الذكية، وأجهزة مراقبة المرضى والأجهزة القابلة للارتداء وغيرها من الأجهزة اللاسلكية" **(World Health Organization, 2011)**
- **تطبيقات الصحة المتنقلة mHealth apps :** هي "برمجيات يتم دمجها في الهواتف الذكية لتقديم وتبادل خدمات الرعاية الصحية للممارسين والباحثين والمرضى"(Chan, 2021).

وتعرفها الباحثة إجرائيا على أنها" تطبيقات تعمل على الهواتف الذكية تهدف إلى توفير معلومات الرعاية الصحية ومساعدة المستخدمين على إدارة صحتهم وحثهم على القيام بسلوكيات صحية إيجابية كالحفاظ على الوزن أو تدعيم النشاط البدني والمدرجة على متاجر التطبيقات في فئتي الطب والصحة واللياقة البدنية.

- **البيانات الشخصية Personal data**: اعتمدت الدراسة التعريف الوارد في المادة الأولى من القانون المصري رقم ١٥١ لسنة ٢٠٢٠ لحماية البيانات الشخصية حيث عرف المشرع البيانات الشخصية على أنها" أي بيانات متعلقة بشخص طبيعي محدد، أو يمكن تحديده بشكل مباشر أو غير مباشر عن طريق الربط بين هذه البيانات وأي بيانات أخرى كالاسم، أو الصوت، أو الصورة، أو رقم تعريفي، أو محدد للهوية عبر الإنترنت، أو أي بيانات تحدد الهوية النفسية، أو الصحية، أو الاقتصادية، أو الثقافية، أو الاجتماعية"**(محكمة النقض المصرية، ٢٠٢٠)**
- **البيانات الشخصية الحساسة Sensitive personal data:** اعتمدت الدراسة أيضا التعريف الوارد في المادة الأولى من القانون المصري رقم ١٥١ لسنة ٢٠٢٠ لحماية البيانات الشخصية حيث عرف المشرع البيانات الحساسة على أنها" البيانات التي تُفصح عن الصحة النفسية أو العقلية أو البدنية أو الجينية، أو بيانات القياسات الحيوية "البيومترية" أو البيانات المالية أو المعتقدات الدينية أو الآراء السياسية أو الحالة الأمنية وفي جميع الأحوال تعد بيانات الأطفال من البيانات الشخصية الحساسة"**(محكمة النقض المصرية، ٢٠٢٠).**

١٠/١ الدراسات السابقة:

حظي موضوع الخصوصية باهتمام العديد من الباحثين، ولكن من زوايا مختلفة (تقنية، وقانونية، وسلوكية)، إلا أنه تبين ندرة الدراسات العربية التي تناولت سياسات الخصوصية لتطبيقات الهواتف الذكية، كما لم تتوصل الباحثة لأية دراسة عربية سبق وأن عالجت قضية الخصوصية بالنسبة لتطبيقات الصحة المتنقلة mHealth apps، وقد قامت الباحثة بعرض بعض من الدراسات ذات الصلة الأكبر بموضوع الدراسة، وجري ترتيبها زمنياً من الأحدث إلي الأقدم (بدءاً من ٢٠٠٩ وحتي٢٠٢٣). وجدير بالذكر أنه لحصر تلك الدراسات قامت الباحثة بالإطلاع على العديد من المصادر مثل:

- **قواعد البيانات العربية** مثل: دار المنظومة، الهادي للإنتاج الفكري(اعلم).
- **قواعد البيانات الأجنبية** المتاحة من خلال بنك المعرفة المصري مثل:(Science Direct, Emerald, Proquest, IEEE, Scopus Database)
- **محركات البحث** مثل: محرك البحث الأكاديمي Google Scholar، ومواقع التواصل الاجتماعي الأكاديمية مثل Research gate.

هذا وقد استخدمت الباحثة مجموعة من المصطلحات البحثية مع اقتصار البحث بها على حقل العنوان و حقل الكلمات المفتاحية وهي كالتالي:

- بالنسبة للمصطلحات العربية استخدمت الباحثة المصطلحات التالية: (الخصوصية المعلوماتية، سياسات الخصوصية، الوعي بالخصوصية المعلوماتية، ممارسات الخصوصية).
- بالنسبة للمصطلحات الأجنبية استخدمت الباحثة المصطلحات التالية (Privacy, Privacy Policy analysis, Privacy Protection, Privacy Awareness, privacy practices, Privacy perception)

وفيما يلي عرض لبعض من الدراسات التي تم حصرها وتقسيمها وفقا لمحورين رئيسيين وهما:

المحور الأول: دراسات اهتمت بتحليل سياسات الخصوصية للمواقع والتطبيقات:

سعت دراسة **(أحمد، ٢٠٠٩)** إلى تحليل سياسات الخصوصية في عينة من محركات البحث العربية وأجنبية واستكشافها بوصفها أهم أداة يمكن من خلالها التعرف إلى رغبة المحرك في الحفاظ على

خصوصية مستخدميه. وكذلك التعرف على القضايا التي عالجتها سياسات الخصوصية، واعتمدت الدراسة على منهج تحليل المضمون، كما استخدمت المنهج المقارن للمقارنة بين المعلومات الواردة في تلك السياسات. ومن أهم النتائج التي توصلت إليها الدراسة أن محركات البحث لديها القدرة على جمع كم هائل من المعلومات من مستخدميها، كما لم تراع السياسات الحد الأدنى من المعايير التي وضعها قانون حماية خصوصية الأطفال على الإنترنت، كما تبين أن سياسات الخصوصية في محركات البحث العربية أضعف بكثير من نظيراتها في المحركات الأجنبية.

أجرى **(Savla & Martino, 2012)** دراسة لتحليل سياسات الخصوصية للشبكات الاجتماعية الصحية. فقد سعت الدراسة لمعرفة مدى امتثال سياسة الخصوصية على الشبكات الاجتماعية الصحية لمبادئ الاستخدام العادل للمعلومات Fair Information Practice(FID) وطبقت الدراسة على ٣٥ شبكة اجتماعية على مستوى الولايات المتحدة، مستخدمة في ذلك منهج تحليل المحتوى لتحليل مضمون سياسات الخصوصية للشبكات الاجتماعية الصحية عينة الدراسة وتقييم سهولة قراءة السياسات وإمكانية الوصول إليها. ومن النتائج التي توصلت إليها الدراسة أن ٩٪ من المواقع لم تتضمن سياسة خصوصية، وأن حوالي ٢٦٪ فقط من مواقع العينة امتثلت لمبادئ FID، ومن ثم أظهرت النتائج أن الامتثال لمبادئ FID كان ضعيفا، وأن غالبية السياسات تتطلب مهارة قراءة أعلى من المتوسط.

هدفت دراسة **(Alhomod & Shafi, 2012)** إلى معرفة ما إذا كانت تتوفر سياسة خصوصية في المواقع الالكترونية الحكومية السعودية، وطبقت الدراسة على ٥٤ موقعا إلكترونيا، وأظهرت النتائج أن ٢٨٪ فقط من المواقع عينة الدراسة لديها سياسة خصوصية على موقعها، كما تبين أن ٦٠٪ فقط من المواقع التي لديها سياسة خصوصية تتوافق سياستها مع مبادئ الاستخدام العادل للمعلومات.

تناولت دراسة **(Moscato, Altschuller & Moscato 2013)** قضية الخصوصية في البيئة المصرفية عبر الانترنت فقد قامت بتحليل وفحص سياسات الخصوصية للمواقع الالكترونية لعدد من البنوك العالمية على شبكة الانترنت بلغ عددها ٢٧٥ مصرفا، وشملت الدراسة الولايات المتحدة وكندا والمكسيك واليابان وأمريكا الجنوبية وأستراليا والصين وأفريقيا، وأظهرت النتائج أن ما يقرب من ثلثي البنوك العالمية لديها بيانات مفصلة للأمن والخصوصية على مواقعها الالكترونية على شبكة الانترنت، بالإضافة إلى أن هناك تباينا طفيفا بين هذه الدول فيما يتعلق ببيانات الخصوصية الموجودة على المواقع الالكترونية لبنوكها على شبكة الانترنت.

سعت دراسة **(Sunyaev, Dehling, Taylor, & Mandl, 2015)** إلى تقييم مدى توافر وشفافية سياسات الخصوصية لتطبيقات الصحة المتنقلة المتاحة على أنظمة ال Android و IOSللخروج بنتائج يمكن أن تساعد العملاء في اتخاذ قرارات حاسمة بشأن استخدام التطبيق أو شراؤه، وأظهرت النتائج أن ٣٠,٥٪ فقط من التطبيقات لديها سياسات خصوصية، وقد كان متوسط طول السياسة ١٧٥٥ كلمة، وقد كانت غالبية ممارسات الخصوصية غير واضحة وغير مفهومة للمستخدمين حيث يتطلب فهمها مستوى عالي من التعليم.

هدفت دراسة **(Lambert, Parke & Bashir, 2015)** إلى تحليل محتوى سياسات الخصوصية لخمسة من أفضل موردى المحتوى الرقمي للمكتبات العامة الأمريكية الذين تربطهم مع المكتبات علاقات تعاقدية لتقديم خدمات معينة مثل استعارة الكتب الالكترونية، أو الكتب الصوتية أو بث الفيديوهات للتأكد من توافقها مع مدونة الأخلاق لجمعية المكتبات الأمريكية ومدى تلبيتها لمعايير الخصوصية لمجتمع المكتبة، وأظهرت النتائج أن سياسات الخصوصية لهؤلاء الموردون تفي إلى حد كبير بمعايير الاستخدام العادل للمعلومات، إلا أنها فشلت في تلبية معايير مجتمع المكتبات، وأوصت الدراسة بضرورة رسم صورة كاملة لكيفية حماية خصوصية المستفيدين في عصر مقدمي الخدمات السحابية.

جاءت فكرة دراسة **(Zimmeck, et al., 2016)** من أن كثيرا ما يلتزم ناشرو التطبيقات بتقديم سياسة خصوصية لإخطار المستخدمين بممارسات الخصوصية في تطبيقاتهم، ولكن هل يتصرف التطبيق حقا كما هو مصرح به في سياسة الخصوصية، حيث تم تطوير نظام آلي لتحليل سياسة الخصوصية ل ١٧٩٩١ تطبيقا مجانيا مع تحليل الشفرة الثابتة لتلك التطبيقات، وأشارت النتائج أن ٧١٪ من التطبيقات تفتقر إلى سياسة خصوصية، وبالنسبة للتطبيقات التي تحتوي على سياسة خصوصية فقد تبين أن ٤١٪ من التطبيقات تجمع معلومات عن الموقع، وأن ١٧٪ تشارك المعلومات مع طرف ثالث دون أن يتم الإفصاح عن ذلك في سياسة الخصوصية، فقد أظهرت النتائج تناقضات بين السياسة وبين ما يتم بالفعل بمتوسط بلغ ١,٨٣.

في ظل اتجاه المكتبات العامة المتزايد إلى الحلول القائمة على الحوسبة السحابية، جاءت دراسة **(Kritikos & Zimmer, 2017)** التجريبية للبحث في كيفية قيام المكتبات العامة بتنفيذ خدمات الحوسبة السحابية لجهات خارجية والتي تعتمد على جمع بيانات المستفيدين، وكيف يمكن أن تؤثر تلك التطبيقات على خصوصية المستفيدين، وكيف تستجيب المكتبات لهذه المخاوف. وقد طبقت الدراسة على ٣٣ مكتبة عامة بالولايات المتحدة الأمريكية مشتركة في خدمة BiblioCommons وهي شركة كندية تطور وتستضيف حلولا برمجية قائمة على الحوسبة السحابية للمكتبات العامة. حيث بحثت الدراسة فيما إذا كانت تلك المكتبات قد قامت بتعديل سياسات وممارسات الخصوصية الخاصة بها عند الاشتراك في هذه الخدمة، وكيف يتم إبلاغ المستفيدين بأي تأثيرات محتملة للخصوصية، وقد كشفت النتائج أن ثماني مكتبات فقط قامت بتعديل سياسة الخصوصية الخاصة بها بعد الاشتراك في خدمات الحوسبة السحابية، وأوصت الدراسة بضرورة تعديل سياسات الخصوصية للمكتبات لتعكس كيفية مشاركة أي معلومات عن المستفيدين مع مزودي الخدمة السحابية، والخطوات التي يتم اتخاذها لحماية خصوصية المستفيد، مع ضمان سهولة وصول المستفيد الي سياسات الخصوصية بتويرها على الصفحة الرئيسية للمكتبة.

جاءت دراسة **(Bowers, Reaves, Sherman, Traynor, & Butler, 2017)** لتكون أول دراسة تقوم بتحليل سياسات الخصوصية ل ٥٤ تطبيق من التطبيقات التي تقدم خدمات المال عبر الهاتف المحمول، تلك التطبيقات التي تصل إلى معلومات هائلة عن العملاء كتاريخ الشراء بالكامل وتحديد الموقع الجغرافي ومعلومات الشبكات الاجتماعية، فقد قامت الدراسة بتحليل مدى توافق سياسات الخصوصية لتلك التطبيقات مع كل من مبادئ الخصوصية للأجهزة المحمولة (GSMA'S Mobile Privacy Principles) وبمعايير المؤسسة الفيدرالية للتأمين على الودائع (the FDIC'S Privacy Rule Handbook)، وأظهرت نتائج الدراسة أن ٤٤٪ من التطبيقات ليس لديها سياسات خصوصية على الإطلاق، كما أن ٥٠٪ من السياسات لم تحدد أبدا للمستخدم البيانات التي يتم تجميعها وتخزينها بالفعل، وأوصت الدراسة بضرورة أن تكون سياسات الخصوصية لخدمات المال عبر الهاتف المحمول واضحة ومكتملة للعمل على حماية خصوصية المستهلك.

تناولت دراسة **(الخثعمي، ٢٠١٧)** سياسات الخصوصية للمواقع الالكترونية للجامعات الحكومية السعودية، لمعرفة مدى توفرها على المواقع الالكترونية، والجوانب التي ركزت عليها، واستخدمت الباحثة المنهج التحليلي وقائمة مراجعة كأداة لجمع البيانات، وتوصلت النتائج أن نسبة ٥٢٪ فقط من إجمالي المواقع الالكترونية للجامعات الحكومية توفر سياسة خصوصية، ومن أبرز الجوانب التي اشتملت عليها سياسات الخصوصية في تلك المواقع هي ملفات تعريف الارتباط، وأوصت الدراسة بضرورة اهتمام الجامعات السعودية بوضع سياسات للخصوصية على مواقعها مع الاهتمام بمراجعتها وتحديثها باستمرار.

قدم **(أحمد، ٢٠١٧)** دراسة لسياسات الخصوصية لمعرفة مدى حماية بيانات مستخدمي شبكات التواصل الاجتماعي المتمثلة في القوانين والتشريعات وتطبيق ذلك في مواقع شبكات التواصل الاجتماعي

بشكل عام، والمكتبات ومؤسسات المعلومات بشكل خاص، عن طريق الإقرارات القانونية وشروط التسجيل والخصوصية المتاحة وسياسات حفظ بيانات المستخدمين ونشرها، بالإضافة إلى زيادة وعي المستفيدين في المكتبات بحماية بياناتهم وكيفية تامين أنفسهم في هذا المجتمع التكنولوجي. ولقد اعتمدت الدراسة على منهج تحليل المحتوى وذلك بتحليل وتفسير القوانين والتشريعات الخاصة بحماية البيانات الشخصية والخصوصية من خلال تحليل مضمون ملفات الخصوصية في مواقع شبكات التواصل الاجتماعي، ومعرفة مدى تطبيق هذه التشريعات والقوانين في مواقع التواصل الاجتماعي للمكتبات المركزية بالجامعات المصرية، وذلك من خلال تصميم قائمة مراجعة وفقا للقوانين والتشريعات التي تحمي وتحفظ البيانات الشخصية والخصوصية، وأوضحت الدراسة عدم إشارة أي من المكتبات عينة الدراسة باتباعها لإجراءات أو سياسات معينة لحماية الخصوصية والبيانات الشخصية، وانتهت الدراسة بوضع تصور مقترح لإنشاء سياسة خاصة بالمكتبات لحماية الخصوصية على مواقع التواصل الاجتماعي الخاصة بها.

سعت دراسة **(Affonso & Sant'Ana, 2018)** لتحليل وفحص قضايا الخصوصية في مرحلة جمع مواقع المكتبات الرقمية الوطنية في أمريكا الجنوبية لبيانات المستخدمين، حيث طُبقت الدراسة على تسع مكتبات وطنية رقمية لتحديد مدى توافر سياسات خصوصية لتلك المكتبات تشرح للمستخدم نوعية البيانات التي تجمعها عنهم ومنهم. والتعرف على نوعية البيانات التي تجمعها هذه المكتبات سواء بعلم المستخدم أو دون علمه، ومدى تأثير تلك النوعية من البيانات على خصوصية المستخدمين. فإن المكتبات الرقمية رغم توفيرها الوصول المجاني للمعلومات إلا أنها تنطوي على مخاطر تتعلق بالخصوصية، فغالبا ما يتطلب هذا النوع من الوصول من المستخدم تعريف نفسه وتفاعله مع البيئة مما يترك آثارا رقمية كافية لاستخدامها في البيئة التجارية أو من قبل الوكالات الحكومية. وتوصلت النتائج أن اثنتين فقط من المكتبات الرقمية الوطنية التي تم فحصها توفر إرشادات الخصوصية وهما المكتبة الرقمية الوطنية في البرازيل والمكتبة الرقمية الوطنية بكولومبيا، وفيما يتعلق بعملية جمع البيانات فقد كانت البيانات التي يتم جمعها دون علم المستخدم تبرز أكثر من البيانات التي يقدمها المستخدم بنفسه. وخلصت الدراسة إلى أن قضايا الخصوصية يمكن أن تتأثر بانخفاض وعي المستخدم بمتى وكيف وأين يتم جمع البيانات، ومن ثم فإن توافر سياسات الخصوصية يصبح ضروريًا في المكتبات الرقمية لزيادة الوعي بهذه العملية.

سعت دراسة **(O'Brien, WH Young, Arlitsch & Benedict, 2018)** لتحليل مدى تطبيق تشفير بروتكول نقل النص التشعبي الآمن (HTTPS) وخدمات تحليلات جوجل Google Analytics على مواقع المكتبات الأكاديمية، ومناقشة الآثار المترتبة على الخصوصية للخدمات المجانية التي تقدم تتبع الويب للمستفيدين، وذلك من خلال تحليل سياسات الخصوصية لعدد ٢٧٩ مكتبة أكاديمية أمريكية ودولية لمكتبات ذات عضوية واحدة أو أكثر في أيا من الاتحادات التالية DLF & ARL, OCLC-RLP، وأشارت النتائج إلى أن نسبة تنفيذ بروتكول HTTPS على مواقع المكتبات الأكاديمية على الويب تمثل ٦٢٪ من بينهم ٣٢٪ تستخدم إعادة توجيه دائمة من HTTP إلى HTTPS لضمان استخدام HTTPS في جميع الاوقات عند الاتصال بالمستفيدين.

جاءت دراسة **(Bachiri, Idri, Fernández-Alemán & Toval, 2018)** لتحليل سياسات الخصوصية للسجلات الطبية الشخصية المتنقلة الخاصة بمراقبة الحمل لدى المرأة وتتبع وإدارة بياناتها الصحية، تلك التطبيقات التي تساعد المستخدمين على تسجيل بياناتهم الطبية وعرضها في أي مكان وفي أي وقت باستخدام الهاتف الذكي، ونظرا لكون هذه البيانات حساسة للغاية مما قد يؤدي إلى أضرار مباشرة وغير مباشرة على المرأة الحامل في حين تم الكشف عنها، كما تسعى الكثير من النساء إلى التشاور من خلال هذه التطبيقات إما للطمأنينة بشأن حملهن أو لأنهن يفتقرن إلى الخبرة أو يرغبن في مشاركة

تجاربهن مع الآخرين مما قد يؤدي إلى الكشف عن معلومات صحية سرية والتي قد تتعرض لهجمات خبيثة من شانها أن تهدد أمن بيانات المرضى وسلامتهم، مما يعني ضرورة أن تكون سياسات الخصوصية دقيقة وحاسمة لتقييد نشر المعلومات الحساسة، حيث تم تقييم سياسات الخصوصية ل ١٩ تطبيق متاحة على نظامي Android و IOS، واظهرت النتائج أن جميع سياسات الخصوصية التي تم تحليلها لا تتوافق تماما مع اللوائح التي تم تحديدها.

قامت دراسة **(Njie, 2018)** بتحليل متعمق للأمان والخصوصية ل ٤٣ تطبيق من تطبيقات الصحة المتنقلة المجانية للتحقيق في مدى امتثالها للوائح حماية البيانات العامة، وقد كشفت النتائج أن غالبية سياسات الخصوصية التي تم تحليلها لا تتبع الممارسات والإرشادات المعروفة حيث لم يتم العثور على أي من التطبيقات بدون مخاطر على الإطلاق. كما تبين أن ٤٠٪ من التطبيقات تنطوي على مخاطر عالية للخصوصية، وأن ٢٨٪ من التطبيقات تنطوي على مخاطر منخفضة للخصوصية، كما تم الكشف عن ثلاث أسباب فنية رئيسية لمخاطر الخصوصية وهي حركة المرور غير المشفرة، والإعلانات المضمنة، ومشاركة البيانات مع طرف ثالث، كما أن ٦٣,٦٪ من التطبيقات يرسلون بيانات غير مشفرة عبر الانترنت، وأن ٨١,٨٪ يستخدمون خدمات تخزين واستضافة تابعة لجهات خارجية مثل خدمات أمازون السحابية.

استهدفت دراسة **(Huckvale, Torous, & Larsen, 2019)** تقييم ممارسات الخصوصية ل ٣٦ تطبيق من أفضل التطبيقات الشائعة للاكتئاب والإقلاع عن التدخين من خلال التقييم النقدي لسياسات الخصوصية وخاصة فيما يتعلق بالكشف عن ممارسات مشاركة البيانات مع أطراف ثالثة، وأسفرت النتائج أن ٦٩٪ من التطبيقات تضمنت سياسة للخصوصية، كما أن ٩٢٪ من التطبيقات التي تشتمل على سياسة للخصوصية ذكرت في سياستها أنها تتشارك البيانات مع طرف ثالث،، كما قام ٢٩ تطبيقا من أصل ٣٦ تطبيق بإرسال البيانات لأغراض الإعلان والتسويق، وأن ١٢ تطبيق كشفوا بيانات المستخدمين لموقع فيسبوك.

هدفت دراسة **(أبو سريع, ٢٠٢٠)** إلى تشخيص واقع عمل تطبيقات جوجل بلاي التي تعمل في بيئة الهواتف الذكية، وخاصة فيما يتعلق بتجميع المعلومات أو السماح بالوصول إلى البيانات والمعلومات الشخصية للمستخدمين، من أجل رصد طبيعة المخاطر المتمثلة في استخدام هذه التطبيقات، حيث قام الباحث بدراسة وتحليل اتفاقيات تراخيص استخدام ٨٠ تطبيقا من تطبيقات الهواتف الذكية تغطي عشرة مجالات، واعتمدت الدراسة على المنهج الوصفي التحليلي المقارن لدراسة وتحليل البيانات التي يتم جمعها أو يطلب السماح بالوصول إليها من قبل تطبيقات الهواتف الذكية، وانتهت الدراسة إلى عدد من النتائج من أهمها أن ٤٥٪ من تطبيقات الهواتف الذكية موضوع الدراسة تعتمد على البرامج الدعائية والإعلانية، كما احتلت تطبيقات التواصل الاجتماعي المرتبة الأولى في جمع المعلومات والبيانات الشخصية الخاصة بالمستخدمين، تلاها في المرتبة الثانية تطبيقات البنوك.

نظرا للاستخدام المتزايد لمرضى السرطان لتطبيقات الصحة المتنقلة للسيطرة على صحتهم فقد جاءت دراسة **(Benjumea, et al., 2020)** لتقييم مدى عدالة سياسة الخصوصية لتطبيقات الصحة المتنقلة الخاصة بالسرطان المتاحة على متجر جوجل بلاي في إسبانيا، حيث قامت الدراسة بتحليل سياسات الخصوصية لتلك التطبيقات بناءً على اللائحة العامة لحماية البيانات، وكشفت النتائج أن ٢٩٪ من التطبيقات ليس لديها سياسة خصوصية، وأن ٣٩٪ من التطبيقات حصلوا على أقل من ٥٠ درجة من أصل ١٠٠ في مقياس الامتثال للوائح وقوانين الخصوصية.

وبسبب الاعتماد المتزايد بالمكتبات الأكاديمية على الموردين الخارجيين للحصول على النظم الآلية لإدارة المكتبات ومجموعاتها، وما يترتب عليه من ضرورة فهم موظفي المكتبة لقضايا الخصوصية وأن

يكونوا على دراية بكيفية استخدام المورد لبيانات المستفيدين حيث أن الخصوصية قيمة أساسية من قيم المكتبات، جاءت دراسة **(McKinno & Turp, 2022)** لتحليل محتوى سياسات الخصوصية لأكثر أربعة أنظمة مستخدمة في المكتبات الأكاديمية بكندا من أجل مساعدة أخصائي المكتبات في فهم سياسات الخصوصية بشكل أفضل ومساعدتهم على اتخاذ قرارات مستنيرة بشأن أنظمة المكتبات الخاصة بهم، وتوصلت الدراسة إلى أن النتائج كانت متشابهة لجميع الموردين، وأن الاختلاف في محتوى السياسات كان طفيفا، وقد حصل نظام SirsiDynix على أقل درجة وهي (٥٥) بينما حصل نظام Ex Libris على أعلى درجة وهي (٥٨).وأوصت الدراسة بضرورة أن تعمل المكتبات والموردون معا لدعم قيم الخصوصية واحترام وحماية حقوق المستخدمين.

وفي ظل اعتماد الحكومات في جميع أنحاء العالم على نظمها الإيكولوجية الرقمية للسيطرة على جائحة كوفيد-١٩، جاءت دراسة **(De & Shukla, 2022)** لتؤكد على ضرورة أن تلتزم الحكومات بنشر ممارسات التعامل مع البيانات لمبادراتهم الرقمية بشكل استباقي من خلال سياسات الخصوصية المناسبة، ومن ثم سعت الدراسة إلى تحليل سياسات الخصوصية لتطبيقات تتبع فيروس كورونا في الهند وذلك بناءً على مدى امتثالها لعشرة مبادئ رئيسية، وطبقت الدراسة على ٦٣ تطبيقا وطنيا متاحة على متجر جوجل بلاي، وأسفرت النتائج أن ٣٨٪ فقط من التطبيقات لديها سياسة خصوصية خاصة بالتطبيق، كما تبين أن صياغة الغرض المحدد لجمع البيانات كان عام في غالبية السياسات مثل : "لتجربة مستخدم أفضل" أو " لتوفير الخدمة وتحسينها"، وحظى تطبيق واحد فقط على مستوى عال من الخصوصية، وأوصت الدراسة بضرورة أن تهتم الحكومة بمعالجة مخاوف الخصوصية بشكل أفضل فيما يتعلق بتطبيقاتها الحالية والمستقبلية لإدارة الكوارث، وضرورة وضع إطار تشريعي شامل لحماية البيانات مع زيادة الوعي بالخصوصية بين المواطنين.

استهدفت دراسة **(كدواني، ٢٠٢٢)** التعرف على مدى الحماية التي توفرها مواقع التواصل الاجتماعي للحق في الخصوصية، بالتطبيق على موقعي فيسبوك وانستجرام.وذلك عبر التحليل الكيفي لمضمون سياسة الخصوصية على الموقعين عينة الدراسة، وكشفت نتائج الدراسة عن تشابه سياسة الخصوصية للموقعين إلى حد كبير، فقد التزمت إدارة موقعي فيسبوك وانستجرم بإعلام المستخدمين بأنواع المعلومات التي تجمعها عنهم، وكيفية مشاركتها مع الآخرين، وخلصت الدراسة إلى حقيقة مؤداها أن مواقع التواصل الاجتماعي تملكها شركات تجارية خاصة، تقدم كثيرا من الخدمات المجانية وتجني أرباحها من جمع بيانات الأفراد ثم تداولها وبيعها إلى طرف ثالث.

سعت دراسة **(المتبولي، ٢٠٢٢)** إلى تقديم إطار نظري عن سياسة حماية خصوصية بيانات المستفيدين من المكتبات في ظل البيئة الرقمية، واستعراض وتحليل سياسات الخصوصية المطروحة بعينة من المكتبات الأجنبية للوقوف على أبرز العناصر الواردة بها، وتقديم نموذج مقترح لعناصر سياسة خصوصية تصلح للتبني والعمل بها في بيئة المكتبات العربية، واستخدمت الدراسة المنهج المسحي بشقيه الوصفي والتحليلي، اعتمادا على قائمة مراجعة طُبقت على تسع مكتبات، ومن أهم النتائج التي توصلت إليها الدراسة عدم اهتمام المكتبات عينة الدراسة في سياساتها بذكر الهدف من وضع سياسة الخصوصية، كما أغفلت معظم المكتبات عنصر خصوصية التعامل مع الأطفال، وأوصت الدراسة بضرورة قيام المكتبات بتوفير بيئة آمنة ومحمية حتى يتمكن المستفيدون من إتاحة معلوماتهم الشخصية بأمان.

المحور الثاني: دراسات اهتمت بدراسة وعي المستخدم بقضايا الخصوصية:

سعت دراسة **(Lawler & Molluzzo, 2010)** إلى تقييم معرفة طلاب الدراسات العليا في جامعة بنيويورك بأبعاد جمع المعلومات وتبادلها في مواقع التواصل الاجتماعي، ومحاولة استكشاف الممارسات الشخصية للطلاب من حيث صلتهم بالخصوصية، وأظهرت النتائج أن ٥٥,٦٪ من المستجيبين لم يقرأوا

سياسة الخصوصية لتلك المواقع لأنها طويلة جدا ومعقدة ومملة، كما أنهم لا يعرفون حقوقهم فيما يتعلق ببياناتهم الشخصية المخزنة على تلك المواقع، وليسوا على دراية بكيفية جمع وتشارك معلوماتهم الشخصية.

تناولت دراسة **(Papathanassopoulos, Athanasiadi & Xenofont, 2016)** كيفية إدارة طلاب جامعة أثينا لخصوصيتهم على موقع فيسبوك، واعتمدت الدراسة على المنهج المسحي الميداني بتطبيق استبانة مقننة على عينة من الطلاب بلغ عددهم ٢٩١ طالب، تراوحت أعمارهم بين ١٨ و٢٦ عاما، وخلصت الدراسة إلى أن الطلاب يستفيدون من وسائل حماية الخصوصية التي يوفرها موقع فيسبوك، كما كشفت الدراسة أن مستخدمي فيسبوك يشعرون أنهم قادرون على استخدام معظم إعدادات الخصوصية لحماية بياناتهم الشخصية، ومع ذلك، فإنهم يشعرون بالقلق إزاء الكشف عن معلوماتهم الشخصية التي تعتبر مسئوليتهم الأساسية.

حاولت دراسة **(Apuru & Andembubtob & Audu Dodoa, 2017)** استكشاف مدى وعي مستخدمي تطبيقات الصحة المتنقلة بخصوصية بياناتهم أثناء استخدام تلك التطبيقات، وقد توصلت الدراسة إلى أن ٤٦٪ من العينة قاموا بتحميل تطبيقات الصحة المتنقلة على هواتفهم، وأن ٨٢٪ منهم يهتمون بقراءة أذونات الوصول التي تطلبها تلك التطبيقات قبل تثبيتها على هواتفهم، كما اهتم ٥٩٪ منهم بقراءة سياسة الخصوصية لتلك التطبيقات، كما قامت الدراسة بتحليل أذونات الوصول التي تتطلبها ٣٥ تطبيق قام أفراد العينة بتثبيتها بالفعل على هواتفهم، والتي كشفت أن نسبة ٨٨,٥٧٪ من تلك التطبيقات طلبت إذن الوصول إلى صور المستخدم والملفات، و٦٥,٧١٪ منها تتطلب إذنا للوصول إلى جهات الاتصال، كما أن ٥٧,١٤٪ من مطوري التطبيقات لا يطلبون صراحة جمع البيانات من المستخدمين على الرغم من أنهم يفعلون ذلك، وخرجت الدراسة بنتيجة مؤداها أن الوعي بالممارسات المسؤولة بين مستخدمي تطبيقات الصحة المتنقلة فيما يتعلق بجمع بياناتهم الشخصية وإدارتها لا يزال منخفضا.

تُعد خصوصية الأفراد مسؤولية مهنية وأخلاقية أساسية لأخصائي المكتبات. فهم يتحملون المسؤولية في حماية خصوصية وكرامة مستخدمي المكتبة، فلكل مستخدم الحق في الخصوصية والسرية. ومن ثم سعت دراسة **(Tummon & McKinnon, 2018)** إلى استكشاف مواقف أخصائي المكتبات الأكاديمية في كندا تجاه الخصوصية، وتحليل تصوراتهم ومواقفهم المتعلقة بممارسات المكتبات المتعلقة بخصوصية المستفيد وسلوكيات الخصوصية عبر الإنترنت بشكل عام. وقد طبقت الدراسة على ١٨٣ من أخصائي المكتبات الأكاديمية الكنديين. وقد تبين من الدراسة أن غالبية أخصائي المكتبات الأكاديمية الكندية يعتقدون أن حماية خصوصية المستفيدين وتثقيفهم حول القضايا المتعلقة بالخصوصية عبر الإنترنت أمر في غاية الاهمية. ومع ذلك فهم لا يرون أن المكتبات تبذل قصارى جهدها لحماية خصوصية المستفيد. وأوصت الدراسة بضرورة أن توجه المكتبات سياساتها وبرامجها المستقبلية للعمل على خلق بيئة يتم فيها حماية حقوق الخصوصية للمستفيدين وتمكن المستفيدين من اتخاذ قرارات مستنيرة حول أفعالهم وممارساتهم عبر الإنترنت.

حاولت دراسة **(النشار، ٢٠١٨)** تقصي مفهوم الخصوصية لدى مستخدمي موقع فيسبوك، من خلال الوقوف على مدى وعيهم بإعدادات الأمان على الموقع، وحدود إفصاحهم من خلاله، ووضوح مخاطر هذا الإفصاح لديهم، وإلى أي مدى تؤثر خبراتهم السابقة على موقفهم منها، وعلاقة كل هذا باتجاهاتهم نحو الفيسبوك، واعتمدت الدراسة على منهج المسح، وذلك باستخدام استمارة استبانة مقننة لجمع البيانات من المبحوثين البالغ عددهم ٤٠٠ مستخدم لموقع فيسبوك ممن تبلغ أعمارهم ١٨ عاما فأكثر، وكشفت نتائج الدراسة أن ٦٧,٢٪ من المبحوثين ذكروا بأنهم تعرضوا لمواقف على الفيسبوك تمثل انتهاكا للخصوصية،

وأن غالبية المبحوثين عينة الدراسة بنسبة ٥٩,٥٪ يمكن وصف فهمهم لإعدادات الأمان على فيسبوك بالمرتفع.

سعت دراسة **(Ali, Rahman & Jahan, 2019)** إلى تقييم مدى الوعي بالأمن والخصوصية بين مستخدمي الهواتف الذكية، ومدى رضاهم الأمني عن الهواتف الذكية، وذلك من خلال منهج المسح، حيث طبقت الدراسة على عينة قوامها ٢٤٩٣ مفردة تتراوح أعمارهم ما بين ٢٠- ٢٦ عاما. وتوصلت الدراسة إلى أن ٢٥,٥٪ من المسجيبين لم يقرأوا أبدا سياسة الخصوصية قبل تثبيت التطبيقات على هواتفهم الذكية، وأن ٥٢,٧٠٪ يقرأوها أحيانا، كما أن ١١,٦٪ لم يقرأوا الأذونات التي يطلبها التطبيق قبل تثبيته على الهاتف، كما تبين أن ٦٠٪ من المستجيبين لا يدركون أمن الهواتف الذكية والخصوصية.

هدفت دراسة **(Shahid & Abdullah, 2020)** إلى تعزيز الوعي حول قضايا الخصوصية والأمن المرتبطة بالشبكات الاجتماعية، وتقديم إرشادات للمستخدمين للاستخدام الآمن للمواقع الاجتماعية، وقد أظهرت نتائج الاستطلاع الذي أجرته الدراسة أن معظم المستخدمين لديهم معلوماتهم الشخصية على مواقع التواصل الاجتماعي، ورغم ذلك فهم لا يغيرون إعدادات الخصوصية لحساباتهم بشكل منتظم، كما يقبل معظم المستخدمين طلبات الصداقة من أشخاص مجهولين، وأوصت الدراسة بضرورة زيادة الوعي بين المستخدمين حول إعدادات الخصوصية، وكيفية التحكم في حساباتهم ونوع المحتوى الذي يجب تحميله على مواقع التواصل الاجتماعي.

جاءت دراسة **(Furini, Mirri, Montangero & Prandi, 2020)** للكشف عن سلوكيات الخصوصية لدى مستخدمي التطبيقات الرقمية والذين يجهلون في الغالب معايير الحماية الرقمية لبياناتهم الشخصية والبيومترية، حيث يقوم المستخدمون في الغالب بتثبيت التطبيقات الترفيهية في أغلب الأوقات دون قراءة شروط وأحكام الاستخدام، والنتيجة هي أن خصوصياتهم في خطر متزايد وأشارت نتائج الدراسة أن تصور المستخدمين تجاه الخصوصية البيومترية أثناء استخدام تطبيقات الهواتف الذكية يتأثر بإدراك ومعرفة البيانات التي تستخدمها التطبيقات المثبتة، كما أشارت النتائج أن الإناث هن أكثر قلقا بشأن احتمال إساءة استخدام كاميرا الهاتف الذكي، وكشفت نتائج الدراسة التحليلية ل ٨٤٣ تطبيقا مثبتا على هواتف الأشخاص عينة الدراسة، أن المستخدمين يتعرضون لانتهاكات خصوصية حيث تصل تلك التطبيقات إلى بيانات حساسة أكثر من اللازم، حيث أن ٢٤٪ من التطبيقات المثبتة تصل إلى جهات الاتصال، و٣٩٪ منها ينتهك خصوصية الموقع ومكان المستخدم، وأن ٥٦٪ من التطبيقات المثبتة لديها حق الوصول إلى الوسائط المتعددة وملفات الصور والفيديو والميكرفون.

استطلعت دراسة **(Avuglah, Owusu-Ansah, Tachie-Donkor & Yeboah, 2020)** مواقف وتصورات ومخاوف أخصائي المكتبات الأكاديمية والطلاب بشأن الخصوصية في البيئة الالكترونية وذلك بالتطبيق في ثلاث جامعات حكومية كبرى في غانا بهدف السعي إلى مواءمة وجهات نظرهم بشكل أفضل، حيث تسعى العديد من المكتبات الأكاديمية إلى دمج عدد من الأدوات والخدمات التكنولوجية في عملياتها لتحسين كفاءة العمل وتقديم الخدمات، والعديد من هذه التكنولوجيات لديها القدرة على تجميع المعلومات الشخصية من المستخدمين مما يمثل انتهاك لخصوصيتهم، وقد اعتمدت الدراسة على الاستبانة كأداة أساسية لجمع البيانات، وقد بلغ عدد المستجيبين (٧٤) من أخصائي المكتبات و(٧٢٦) طالبا. وأشارت النتائج أن ٧٥,٧٪ من أمناء المكتبات و ٨٦,٥٪ من الطلاب موافقون بشدة على أن الأفراد يجب أن يكونوا قادرين على التحكم في من يرى معلوماتهم الشخصية، كما أن ٧١,٦٪ من أمناء المكتبات و ٨٠,٩٪ من الطلاب يرون أنه لا ينبغي على المكتبات أبدا تقاسم المعلومات الشخصية أو سجلات الإعارة أو سجلات استخدام الانترنت مع أطراف ثالثة ما لم يأذن بها الفرد، كما أظهر غالبية المستجيبون موقفا إيجابيا تجاه دور المكتبة في تعليم الخصوصية وأن أمناء المكتبات يجب أن يلعبوا دورا في تثقيف

الطلاب بشأن مخاطر الخصوصية المحتملة عند استخدام الانترنت، وأوصت الدراسة بضرورة أن يدمج أخصائي المكتبات الأكاديمية الغانية تعليم الخصوصية كجزء من جهودهم التعليمية، وضرورة أن يثبتوا صراحة بأنهم قادرون على الحفاظ على قدسية بيانات المستفيدين من خلال تطوير قوانين حماية البيانات في سياسات الخصوصية بالمكتبات.

سعت دراسة **(Havelka, 2021)** إلى بحث ومقارنة سلوك الخصوصية لمستخدمي الهواتف الذكية من طلاب علوم المكتبات والمعلومات في جامعتين (جامعة ولاية نيوجرسي بالولايات المتحدة وجامعة برلين بألمانيا)، وذلك من خلال المقابلة الشخصية مع عينة من الطلاب، وكشفت النتائج أنه لا توجد اختلافات ثقافية في سلوك خصوصية الهاتف المحمول بين المشاركين في الدراسة، بينما أوصت الدراسة بضرورة العمل لزيادة الوعي بالخصوصية خاصة فيما يتعلق بالحوسبة المتنقلة والتقنيات الناشئة والذكاء الاصطناعي.

كشفت دراسة **(سليمان،٢٠٢١)** عن مدى وعي أعضاء هيئة التدريس ومعاونيهم بجامعة جنوب الوادي ببنود سياسة الخصوصية بمواقع التواصل الاجتماعي، وتحديد مدى وعيهم بسياسات وضوابط تخزين البيانات عبر الأجهزة المستخدمة للولوج إلى مواقع التواصل الاجتماعي، ومعرفة مدى تأثير بنود سياسة الخصوصية على التفاعل والتشارك المعرفي لديهم، واعتمدت الدراسة على المنهج الميداني واستخدمت الاستبانة الالكترونية كأداة لجمع البيانات عن مجتمع الدراسة الذي بلغ (٣١٧)عضوًا، وكشفت النتائج أن ٥٤,٣٪ من العينة يرون أن السياسات والضوابط المتعلقة بتخزين البيانات الشخصية في مواقع التواصل الاجتماعي تتسم بالغموض وعدم الوضوح، كما أن مواقع التواصل الاجتماعي لا تقوم بإعلامهم بالتغيرات التي تطرأ على سياسة أمن وتخزين بيانات الخصوصية.

أكدت دراسة **(Albatat, Clar & Abulkhair, 2023)** على تزايد اعتماد خدمات الرعاية الصحية القائمة على إنترنت الأشياء على بيانات المستخدمين الشخصية والحساسة، ومن ثم أصبح وعي المستخدمين بقضايا الخصوصية ضروري عند استخدام هذه الأنظمة. لذا سعت الدراسة إلى اكتشاف مستوى الوعي بالخصوصية بين مستخدمي خدمات الرعاية الصحية بالسعودية لتحديد مدى قدرتهم على إدارة خصوصيتهم ضمن خدمات الرعاية الصحية القائمة على إنترنت الأشياء، وتوصلت الدراسة إلى أن ٤,٦٪ من المستجيبين لديهم وعي عال، وأن غالبية المستجيبين بنسبة ٧٢,٣٪ لديهم وعي متوسط، و٢٣,١٪ لديهم وعي منخفض.

التعقيب على الدراسات السابقة:

بعد العرض السريع للدراسات العربية والأجنبية في مجال سياسات الخصوصية والوعي بالخصوصية في البيئة الرقمية، يتبين عدد من الجوانب الهامة:

- هناك اهتمام متزايد بقضايا الخصوصية نظرا لكونها من المجالات البحثية الحديثة المرتبطة بالتطورات الخاصة بالمواقع والتطبيقات على شبكة الإنترنت.
- ولدت تكنولوجيا المعلومات والاتصالات وتكنولوجيا الهواتف الذكية مجموعة كبيرة من تحديات الخصوصية، والدليل على ذلك تنوع فئات المواقع الالكترونية والتطبيقات التي تم تحليل سياسات الخصوصية الخاصة بها لأنها تتعامل مع بيانات شخصية وحساسة للمستخدمين مثل (مواقع البنوك، مواقع التواصل الاجتماعي، مواقع المكتبات، مواقع حكومية، مواقع جامعات، تطبيقات الهواتف الذكية).

- أكدت غالبية الدراسات أن معرفة وفهم لوائح الخصوصية يمكن أن يؤثر على وعي المستخدمين مما يساعدهم في اتخاذ القرارات المناسبة فيما يتعلق ببياناتهم الحساسة والشخصية عند التفاعل مع أي نظام أو التعامل معه.
- اعتمدت غالبية الدراسات على منهج تحليل المضمون لتحليل سياسات الخصوصية للمواقع والتطبيقات، بينما اعتمدت الدراسات التي اهتمت برصد ممارسات الخصوصية لدى المستخدمين على المنهج المسحي.
- تشابهت الدراسة الحالية مع بعض الدراسات السابقة في تركيزها على تحليل سياسات الخصوصية لتطبيقات الصحة المتنقلة مثل دراسة (Sunyaev, Dehling, Taylor, & Mandl, 2015) و دراسة (Bachiri, Idri, Fernández-Alemán & Toval, 2018) و دراسة (Njie, 2018) و دراسة (Huckvale, Torous, & Larsen, 2019) ودراسة (Benjumea, Ropero, Rivera-Romero, Dorronzoro-Zubiete, & Carrasco, 2020)، ولكن تختلف معها في أن تلك الدراسات ركزت على تطبيقات صحية معينة كتلك الخاصة بالاكتئاب أو الإقلاع عن التدخين أو الحمل أو مرضى السرطان وذلك في أماكن معينة كاستراليا وأسبانيا، في حين ركزت تلك الدراسة الحالية على تطبيقات الصحة المتنقلة المجانية الأكثر رواجا على النسخة المصرية من متجر جوجل بلاي بغض النظر عن الفئة الموجهة لها.
- تتميز الدراسة الحالية بأنها تُعد أول دراسة عربية تهتم بتحليل سياسات الخصوصية لتطبيقات الصحة المتنقلة، وترصد مدى الوعي بالخصوصية بين مستخدمي تلك التطبيقات في مصر.
- أفادت الباحثة من الدراسات السابقة في مناقشة النتائج التي توصلت إليها الدراسة الحالية.

ثانيا: الجانب النظري للدراسة:

١/٢ مفهوم الخصوصية المعلوماتية:

نظرا لما أحدثته الإنترنت من ثورة في عالم الاتصالات، حيث أصبحت وسيلة الاتصال المفضلة. يتسوق الناس ويتبادلون الصور والرسائل ويتعلمون ويعملون وحتى يتلقون الاستشارات الطبية عبر الإنترنت**(Pitkänen & Tuunainen, 2012)**، وهو ما أثار مخاوف بشأن الخصوصية، فمع نمو البيانات أصبحت مهمة حماية الخصوصية والأمن عبر الإنترنت أكثر تعقيدا، وأصبح الحق في الخصوصية من أكثر الحقوق عرضة للانتهاك في البيئة الرقمية. ومن ثم أصبحت التعريفات التقليدية للخصوصية التي تم صياغتها قبل ظهور الإنترنت ليست مجهزة للتعامل مع التحديات التي تجلبها التكنولوجيا، مما أدى إلى استنتاج أن مفهوم الخصوصية متعدد الأبعاد **(Katulić, 2023)**. وقد حاولت مؤسسة الخصوصية الدولية International Association of Privacy أن تضفي شيئاً من الوضوح على هذه المسألة من خلال تعريف الخصوصية بأنواعها المختلفة وهي**(اليونسكو، ٢٠١٣):**

- **الخصوصية الجسدية أو المادية Bodily Privacy:** وتتعلق بالحماية ضد أي اعتداءات تمس النواحي الجسدية مثل فحوصات الجينات وفحص المخدرات والمؤثرات العقلية.
- **خصوصية الاتصالات Communications Privacy**: وتعني بسرية وخصوصية الاتصالات والمراسلات الهاتفية والبريد الالكتروني وغيرها من الاتصالات.
- **الخصوصية المكانية أو الإقليمية Territorial privacy**: والتي تتعلق بالقواعد المنظمة للدخول إلى المنازل وبيئة العمل أو الأماكن العامة والتي تتضمن التفتيش والرقابة الإلكترونية.

- **الخصوصية المعلوماتية Information Privacy**: والتي تتعلق بالقواعد التي تحكم جمع وإدارة البيانات الخاصة (معلومات طبية، معلومات مالية، بطاقات الهوية). والتي هي موضع اهتمام هذه الدراسة.

وفي إطار تحديد مفهوم خصوصية المعلومات، تجدر الإشارة أنه في نهاية الستينيات والسبعينيات أثير لأول مرة المصطلح كمفهوم مستقل عن بقية مفاهيم الخصوصية، وذلك من خلال فقيهين أمريكيين، الأول ألان ويستن Alan Westin عام ١٩٦٧ والذي عرفها على أنها" "حق الأفراد في تحديد متى وكيف وإلى أي مدى تصل المعلومات عنهم للآخرين" أما الثاني ميلر Miller عام ١٩٧١والذي عرفها على أنها " قدرة الأفراد في التحكم بدورة المعلومات التي تتعلق بهم"**(مصطفى، ٢٠١٦)**. وعليه ارتبط مفهوم الخصوصية المعلوماتية بمفهوم حماية المعلومات. وأصبح مصطلح الخصوصية في بيئة مواقع الانترنت يشير إلى حماية الخصوصية المعلوماتية أو حماية البيانات، ومن ثم عُرف الحق في الخصوصية على الانترنت بأنه" حق الفرد في أن يضبط عملية جمع المعلومات الشخصية عنه، وعملية معالجتها وحفظها واستخدامها في صنع القرار الخاص به أو المؤثر فيه، ومن ثم الحق في الإطلاع عليها، وتصحيحها إذا كانت غير صحيحة ومحوها إذا كانت محظورة**(كدواني، ٢٠٢٢)**.

ومن ثم يمكن القول أن الحق في الخصوصية في البيئة الرقمية بصفته حقا أصيلا من حقوق الإنسان، يتكون من عدة حقوق فرعية أهمها **(أحمد، ٢٠١١)**:

- **الحق في التخفي الرقمي**: ويعني أن لكل شخص الحق في التواجد على شبكة الانترنت دون أن يكون مجبرا على كشف هويته الحقيقية شرط ألا يضر ذلك بالنظام العام وحقوق وحريات الغير.
- **الحق في النسيان الرقمي**: ويعني أن يلتزم المسؤولون عن معالجة البيانات الشخصية بعدم حفظ البيانات لمدة تتجاوز الغاية التي جمعت من أجلها، كما يعني ذلك أن لكل شخص الحق في تعديل أو حتى سحب معلومات تخصه من شبكة الانترنت شرط ألا يحدث ذلك ضررا للأشخاص الذين بحوزتهم هذه المعلومات.
- **الحق في الهوية الرقمية**: ويعني أن يكون لكل شخص الحق في التواجد كشخص رقمي على شبكة الانترنت، إلى جانب وجوده كشخص حقيقي.

٢/٢ الخصوصية والهواتف الذكية:

رغم ما أحدثته الثورة التكنولوجية من آثار إيجابية، إلا أن هذا التطور في وسائل تكنولوجيا المعلومات والاتصالات أفرز العديد من المخاطر التي تواجه الحق في حرمة الحياة الخاصة، فإن سهولة عمليات التخزين والمعالجة الالكترونية وازدياد تدفق المعلومات، كل ذلك تسبب في ضعف قدرة الفرد على التحكم في بياناته الخاصة **(Havelka, 2021)**.

ومع التطور وبظهور الهواتف الذكية لم يعد الهاتف مجرد وسيلة اتصالية فقط، بل تعددت استخداماته وتطبيقاته التي فرضت نفسها على جميع أوجه الحياة وأحدثت تغيرات في جميع مناحي الحياة الإنسانية والاجتماعية، وذلك لما تقوم به من مهام خاصة بنقل وإرسال واستقبال مختلف المعلومات والبيانات **(أبو سريع، ٢٠٢٠)**.

لقد تسببت ثورة استخدام الانترنت عبر الهواتف الذكية واستخدام الأفراد المتزايد للتكنولوجيا الرقمية في الكثير من المخاوف حول حماية الخصوصية والبيانات، والتي يمكن تحليلها من خلال أربعة عوامل: كمية المعلومات التي تجمعها الأجهزة والتقنيات الرقمية؛ السرعة التي يمكن بها مشاركة المعلومات؛ طول مدة التخزين ونوع المعلومات التي يمكن جمعها، حيث تمتد تهديدات الخصوصية من اللحظة التي ينقل فيها

المستخدم نشاطه إلى وسيط رقمي ويترك آثار التفاعل في تلك البيئات **(Affonso & Sant'Ana, 2018)**. حيث تحولت البيانات الشخصية إلى سلعة يتم استخدامها إما تجاريا في تنفيذ دعاية تسويقية، أو استغلالها في أغراض تضر بأصحابها. وعادة ما يتبادر إلى الذهن تساؤل مهم ألا وهو: إلى أين تذهب البيانات والمعلومات الشخصية بعد تقديم الخدمة وانقضائها؟ هل تحتفظ المواقع والتطبيقات ببياناتنا الشخصية؟ وإذا كان الأمر كذلك فأين تذهب تلك البيانات وكيف يتم استخدامها فيما بعد؟

ويرى **(Yerukhimovich, et al., 2016)** أنه يجب أن يبدأ أي نقاش حول مشكلة الخصوصية على الهاتف الذكي بفهم كامل لأبعاد المشكلة. أولا: الهاتف نفسه والذي يمتلك قدرات تكنولوجية ومستشعرات مختلفة قادرة على جمع المعلومات. ثانيا، لابد من النظر إلى الوظيفة أو الفائدة التي يريد المستخدمون الحصول عليها عند استخدامهم هذا الهاتف، فضلا عن نوعية المعلومات التي ستجمع وتستخدم، وأخيرا ينبغي النظر أيضا إلى مقدمي مختلف الخدمات الموجودة على الهاتف، تشمل القائمة هنا مصنعي الهاتف، ومصممي نظام لتشغيل، وشركات الاتصالات، ومطوري التطبيقات وتختلف الطريقة التي تكسب بها كل مجموعة المال من الخدمات التي تقدمها اختلافا كبيرا ولكل واحدة منها تبعات مختلفة على خصوصية المستخدم.

وقد شهدت السنوات الأخيرة زيادة كبيرة في عملية استغلال إمكانيات الهواتف الذكية من قبل متخصصي الرعاية الصحية، فأصبحت تطبيقات الصحة المتنقلة سوقا مزدهرا لا يستهدف المرضى والأطباء فقط بل أيضا أولئك الذين لديهم اهتمام بالصحة واللياقة البدنية ففي عام ٢٠١٨ قام ٦٠٪ من مستخدمي الهواتف الذكية بتثبيت تطبيقات الصحة المتنقلة على هواتفهم، إلا أنها تطرح مشكلات تتعلق بالخصوصية بسبب البيانات الشخصية والحساسة التي يمكنها الوصول إليها، فعند استخدام تلك التطبيقات يحتاج المستخدم إلى إدخال الكثير من البيانات الشخصية، وقد تؤدي معالجة البيانات الشخصية إلى مخاطر على حقوق الأفراد وحرياتهم، ولهذا توفر قوانين ولوائح الخصوصية لأصحاب البيانات حقوقا كما تفرض على معالجي ومراقبي البيانات التزامات **(Liu, Sun & Zheng, 2018)**. فلابد أن يلتزم مطورو تطبيقات الصحة المتنقلة بمعالجة البيانات الشخصية والحساسة بطريقة أخلاقية وقانونية مع الكشف عن ممارساتهم في ذلك بمنتهى الشفافية، فإن أحد مبادئ حماية البيانات وفقا للائحة العامة لحماية البيانات هو مبدأ الشفافية، بمعنى أن تكون الممارسات شفافة للأفراد في كيفية جمع بياناتهم الشخصية أو استخدامها، أو معالجتها، أو إتاحتها، بما في ذلك المعلومات المرتبطة بفترات الاحتفاظ بالبيانات ومشاركتها مع جهات أخرى**(Katulić, 2023)**.

٣/٢ الاهتمام التشريعي بالخصوصية:

إن الخصوصية هي حق إنساني أساسي، منصوص عليه في جميع الصكوك الدولية والإقليمية لحقوق الإنسان، كما حظي موضوع الحق في الخصوصية باهتمام تشريعي سواء على المستوى الدولي أو القومي، فهو كان ومازال موضع اهتمام مُشرعي القوانين، وقد كان إطار مبادئ ممارسة المعلومات العادلة Fair Information Practice Principles أحد الأطر المستخدمة لفترة طويلة لفهم لوائح الخصوصية وتحديدها، والتي يتم استخدامها لتقييم أنظمة المعلومات والبرامج والأنشطة التي تؤثر على الخصوصية وتتمثل تلك المبادئ في الآتي **(Alhomod & Shafi, 2012)**:

- **الإشعار Notice** : يجب على جامعي البيانات الكشف عن ممارساتهم المتعلقة بجمع المعلومات قبل البدء بجمع المعلومات الشخصية من المستخدمين.

- **الاختيار Choice :** يجب أن يعطي المستخدمون الخيار في إذا ما كانوا يرغبون في أن تجمع معلوماتهم الشخصية أم لا، وكيفية استخدامها والغايات التي ستستخدم فيها إن كانت ستتجاوز تلك التي جمعت لأجلها في المقام الأول.
- **الوصول Access :** يجب أن يتمكن المستخدمون من رؤية البيانات التي جمعت عنهم والتحقق من دقتها واكتمالها.
- **الأمن Security:** يجب على جامعي البيانات اتخاذ خطوات معقولة لضمان أمان وسلامة المعلومات التي تجمع عن المستخدمين وحمايتها من أي استخدام غير مصرح به.
- **الإنفاذ Enforcement :** استخدام آلية موثوقة لفرض عقوبات تجاه عدم الامتثال لمبادئ ممارسة المعلومات العادلة.

كما حظيت مسألة حماية البيانات الشخصية بعد التقدم الكبير الذي تم إحرازه في مجال تكنولوجيا الاتصالات والمعلومات بالكثير من اهتمام دول العالم ففي الاتحاد الأوربي وفي الولايات المتحدة تبنت قوانين الخصوصية الحديثة مفهوما للخصوصية يرتبط بشكل أساسي بالتحكم في جمع المعلومات الشخصية وتخزينها واستخدامها، وما يؤكد ذلك صدور اللائحة العامة لحماية البيانات الشخصية General Data Protection Regulation(GDPR) الخاصة بدول الاتحاد الأوربي، وهي عبارة عن مجموعة من القوانين والقواعد تتعلق بالخصوصية تمت الموافقة عليها في إبريل ٢٠١٦ من قبل المفوضية الاوربية لحماية حقوق جميع مواطني الاتحاد الأوربي وبياناتهم الشخصية ليحل محل التوجيه رقم EC 95/46 الصادر عن البرلمان الأوربي في ٢٤ أكتوبر ١٩٩٥ بشأن حماية الأفراد فيما يتعلق بمعالجة بياناتهم الشخصية وحرية حركة تلك البيانات **(يس؛ السيد، ٢٠٢٢)**، حيث تعزز اللائحة العامة لحماية البيانات جميع مبادئ حماية البيانات والالتزامات والحقوق المنصوص عليها في التوجيه، فضلا عن ما تتضمنه من آليات حماية إضافية للسماح للأفراد بالتحكم بشكل أفضل في بياناتهم الشخصية، وهو ما يمثل تحديًا بشكل خاص في بيئة الإنترنت والهواتف الذكية **(Bailey, 2018)**.

كما اعتمدت الجمعية العامة للأمم المتحدة في ديسمبر ٢٠١٣ القرار ٦٨/ ١٦٧ بشأن الحق في الخصوصية في العصر الرقمي ودعت جميع الدول للالتزام بواجباتهم في احترام وحماية الحق في الخصوصية الرقمية عبر الإنترنت **(مكاوي، ٢٠٢٢)**. وكخطوة لضبط الأمن المعلوماتي في مصر صدر القانون رقم ١٥١ لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية وتنظيم التعامل فيها، والذي يعد بمثابة انطلاقة تشريعية نحو تأمين البيانات الشخصية للمواطنين.

وقد أكدت اللائحة العامة لحماية البيانات ومن بعدها جميع لوائح وقوانين الخصوصية على ضرورة أن يحتفظ الشخص المعني بالبيانات بالحقوق التالية لحماية بياناته الشخصية **(Bailey, 2018)**:

- **الحق في الوصول Right of access:** يجوز للشخص أن يطلب التأكد من ماهية المعلومات التي يتم حفظها وتخزينها ويطلب نسخة منها، كما يحق له الوصول إلى أغراض المعالجة.
- **الحق في التصحيح Right of rectification**: للشخص أن يطلب تصحيح وتحديث البيانات إذا كانت غير دقيقة.
- **الحق في قابلية نقل البيانات Right of data portability :** للشخص أن يطلب نقل البيانات من مزود خدمة إلى آخر.
- **الحق في تقييد المعالجة Right of restriction:** في بعض المواقع من حق الشخص أن يطلب تقييد نطاق المعالجة إذا كان هناك خلاف حول وقتها أو استخدامها المشروع.

- **الحق في الاعتراض Right to object :** للشخص الحق في الاعتراض على معالجة بياناته الشخصية في حال إذا كانت المعالجة لالتزام قانوني أو مالي أو تعاقدي أو تسويقي.
- **الحق في المحو Right to Erasure:** أو بمعنى آخر الحق في النسيان الرقمي، ففي بعض الحالات يمكن للشخص أن يطلب محو البيانات الشخصية إذا لم يكن هناك أسباب قانونية للاحتفاظ بهذه البيانات.

ثالثا: الجانب التطبيقي للدراسة:

يناقش هذا الجانب النتائج التي توصلت إليها الباحثة من تحليل سياسات الخصوصية لتطبيقات الصحة المتنقلة عينة الدراسة، وكذلك نتائج الدراسة الميدانية التي طبقت على عينة من مستخدمي تلك التطبيقات بمصر.

١/٣ أساليب التحليل الإحصائي والمعاملات الإحصائية:

تم إدخال البيانات ومعالجتها باستخدام برنامج Excel واستخدام الاختبارات والمعالجات الإحصائية التالية:

- حساب التكرارات والنسب المئوية لجميع محاور قائمة المراجعة وأسئلة الاستبانة.
- استخراج المتوسط الحسابي لدرجة بنود كل محور، فيما يخص محاور قائمة المراجعة.
- حساب متوسط الوزن النسبي الفارق لتحديد درجة توافر كل محور من محاور قائمة المراجعة، وسؤال ممارسات الخصوصية وآليات الحماية بالاستبانة، حسب المقياس الثلاثي، حيث (١، ٠,٥، ٠) تمثل قيم الوزن النسبي على التوالي، وتم تحديد درجة كل مؤشر حسب المعيار التالي(درجة قيمة كل فئة = (أعلى قيمة - أقل قيمة)/ عدد البدائل)=(١-٠)/٣)= ٠,٣٣، ليصبح طول الخلايا في المقياس الثلاثي كما يلي:

طول الخلية	٠.٦٨ إلى ١	٠.٣٤ إلى ٠.٦٧	٠ إلى ٠.٣٣
الوزن	١	٠.٥	٠
مستوى الامتثال لأفضل ممارسات الخصوصية	عال	متوسط	ضعيف

- لتصنيف تطبيقات الصحة المتنقلة عينة الدراسة وفقا لاحتمالية مخاطر الخصوصية بها، حيث أن الامتثال للقوانين والشفافية في الكشف عن ممارسات الخصوصية من الممكن اعتباره مؤشرا لحُسن نية مقدمو الخدمة في حماية البيانات الشخصية والحساسة للمستخدمين، فيمكن توضيحها كما يلي:

درجة امتثال التطبيقات لبنود قائمة المراجعة	أقل من ٣٠٪	من ٣٠٪ إلى أقل من ٥٠٪	من ٥٠٪ إلى ٧٥٪	أكثر من ٧٥٪
المستوى	ذات مخاطر خصوصية مرتفعة جدا	ذات مخاطر خصوصية مرتفعة	ذات مخاطر خصوصية متوسطة	ذات مخاطر خصوصية منخفضة

٢/٣ الدراسة التحليلية لسياسات الخصوصية لتطبيقات الصحة المتنقلة عينة الدراسة:

تقوم الباحثة في هذا الجزء بتحليل البيانات الواردة في قائمة المراجعة وتحليل محتوى سياسات الخصوصية لتطبيقات الصحة المتنقلة عينة الدراسة للتأكد من امتثالها للوائح وقوانين الخصوصية، حيث

تشُكل معالجة البيانات الشخصية بالتوافق مع هذه اللوائح والقوانين أمرا ضروريا من أجل الممارسة الجيدة لحماية البيانات.

ويوضح الجدول رقم (٢) مدى امتثال مقدمو الخدمة بتطبيقات الصحة المتنقلة للوائح وقوانين الخصوصية ومدى التزامهم بالكشف عن ممارساتهم حيال خصوصية المستخدمين، حيث يتضح أن مستوى امتثالهم لقوانين الخصوصية وكشفهم عن ممارساتهم كان ضيعفا بمتوسط حسابي بلغ (٠,٣٢)، ومعني ذلك أن مقدمو الخدمة لتطبيقات الصحة المتنقلة عينة الدراسة لم يطبقوا بالشكل الكاف أفضل الممارسات المسؤولة عند جمع ومعالجة ومشاركة بيانات المستخدمين الشخصية والحساسة، مما يجعل سياسات الخصوصية غير شفافة للمستخدمين فهي لم تحقق الهدف المنشود منها، حيث جاءت غير مستوفية للشروط.

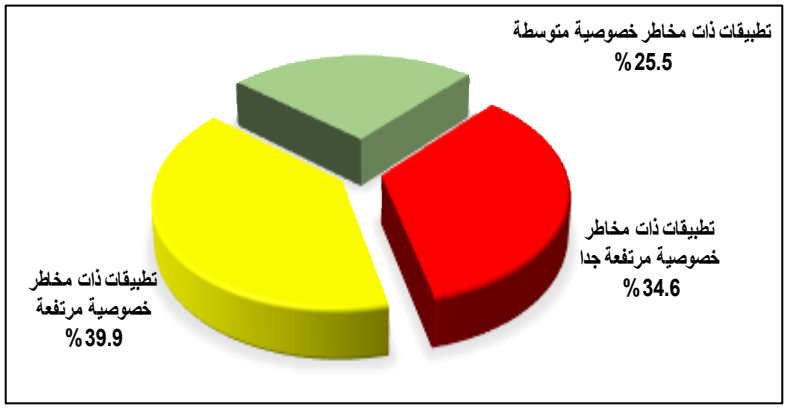
جدول رقم (٢): مستوى امتثال تطبيقات الصحة المتنقلة عينة الدراسة لأفضل ممارسات حماية البيانات الشخصية للمستخدمين

المحاور	المتوسط الحسابي	مستوى الامتثال
قواعد وممارسات عامة	0.34	متوسط
جمع البيانات	0.34	متوسط
أغراض جمع وتحليل البيانات	0.44	متوسط
مشاركة البيانات مع أطراف ثالثة	0.44	متوسط
تأمين البيانات	0.20	ضعيف
حق المستخدم وسيطرته على بياناته	0.43	متوسط
الإبلاغ عن تحديث أو تعديل سياسة الخصوصية	0.32	ضعيف
الإبلاغ عن تسريب البيانات	0.03	ضعيف
المتوسط الحسابي العام	0.32	ضعيف

حيث جاء تطبيق مقدمو الخدمة لتطبيقات الصحة المتنقلة لأفضل ممارسات حماية البيانات الشخصية متوسطا في بعض المحاور، ويأتي في مقدمتها محوري "أغراض جمع وتحليل البيانات" و"مشاركة البيانات مع أطراف ثالثة" بمتوسط حسابي بلغ(٠,٤٤) لكل منهما، تلا ذلك في المرتبة الثانية محور"حق المستخدم وسيطرته على بياناته" بمتوسط حسابي بلغ(٠,٤٣)، وفي المرتبة الثالثة جاء محوري" القواعد والممارسات العامة" و" جمع البيانات" بمتوسط حسابي بلغ (٠,٣٤) لكل منهما.

بينما جاء تطبيقهم لأفضل الممارسات ضعيفا في ثلاث محاور، وهي محور"الإبلاغ عن تحديث أو تعديل سياسة الخصوصية" بمتوسط حسابي بلغ (٠,٣٢)، تلا ذلك محور" تأمين البيانات" بمتوسط حسابي بلغ (٠,٢٠)، وأخيرا محور" الإبلاغ عن تسريب البيانات" بمتوسط حسابي بلغ (٠,٠٣).

كما يتبين من الشكل رقم (١) أن هناك (٦١) تطبيق بنسبة (٣٩,٩٪) تم تصنيفها وفقا للمقياس الذي وضعته الدراسة على أنها ذات مخاطر خصوصية مرتفعة، بينما صُنف (٥٣) تطبيق بنسبة(٣٤,٦٪) بأنها ذات مخاطر خصوصية مرتفعة جدا، وتم تصنيف (٣٩) تطبيق بنسبة (٢٥,٥٪) بأنها ذات مخاطر خصوصية متوسطة، بينما لم يُصنف أيا من التطبيقات عينة الدراسة بأنه ذات مخاطر خصوصية منخفضة.



شكل رقم (١): تصنيف تطبيقات الصحة المتنقلة عينة الدراسة وفقا لمستوى احتمالية مخاطر الخصوصية بها

وتستعرض الدراسة فيما يلي نتائج تحليل سياسات الخصوصية لتطبيقات الصحة المتنقلة عينة الدراسة بمزيد من التفصيل، ولكن هناك بعض الملاحظات التي ينبغي الإشارة إليها قبل ذلك، وهي:

- تشابه سياسات الخصوصية في كثير من التطبيقات، وكأنها قالب جاهز يتم الاستعانة به.
- أن بعض سياسات الخصوصية جاءت مختصرة بطريقة مبالغ فيها، والذي أرجعته الباحثة إلى كون مطورو التطبيق مجبرين على تضمين التطبيق لصفحة سياسة الخصوصية حتى يتم إدراجه على متجر جوجل بلاي.
- فيما يتعلق بالأذونات التي تطلبها التطبيقات، فقد جاءت الأذونات المذكورة في سياسات الخصوصية لبعض التطبيقات أكثر من الأذونات التي يقدمها المتجر في معلوماته عن التطبيق، مما يعني أن المعلومات التي يوفرها المتجر عن التطبيقات غير كافية ولا يجب أن يعتمد عليها المستخدم في اتخاذ القرار حول تثبيت التطبيق من عدمه، بل لابد أن يطلع على بنود سياسة الخصوصية.

أولا: قواعد وممارسات عامة:

إن الغرض من سياسات الخصوصية هو إبلاغ المستخدمين بالبيانات التي تجمعها التطبيقات والمواقع منهم وعنهم، وكيفية استخدام مقدمو الخدمة لها وتخزينها ومعالجتها وتأمينها أيضا، وحيث أن هذه السياسات موجهه في الأساس لجميع المستخدمين على اختلاف فئاتهم ومستواهم التعليمي، لذا لابد أن تكون مكتوبة بلغة واضحة وسهلة الفهم، بحيث تكون أداة لمعالجة مخاوف الخصوصية لدى المستخدمين، ويوضح جدول رقم (٣) بعض البنود والممارسات العامة التي يجب توافرها في سياسات الخصوصية لتطبيقات الصحة المتنقلة عينة الدراسة.

جدول رقم (٣): مستوى امتثال تطبيقات الصحة المتنقلة عينة الدراسة للقواعد والممارسات العامة

البنود	نعم		جزئيا		لا		المتوسط الحسابي	الترتيب
	ت	النسبة٪	ت	النسبة٪	ت	النسبة٪		
تتسم نصوص سياسة الخصوصية بالوضوح وسهولة الفهم من قبل المستخدم	35	22.9%	40	26.1%	78	51.0%	0.36	3
سياسة الخصوصية متاحة بأكثر من لغة من ضمنها اللغة العربية	16	10.5%			137	89.5%	0.10	7
تتضمن سياسة الخصوصية على تعريفات واضحة وغير قابلة للتأويل لجميع المصطلحات القانونية والتقنية المستخدمة في بنود الخصوصية.	22	14.4%	15	9.8%	116	75.8%	0.19	5
هناك وسيلة للتواصل بين المستخدم ومقدم الخدمة للرد على التساؤلات الخاصة بحماية الخصوصية.	127	83.0%			26	17.0%	0.83	1
تنص سياسة الخصوصية على تمكين المستخدم من خيارات رفض أو قبول استخدام ملفات تعريف الارتباط في التطبيق			104	68.0%	49	32.0%	0.34	4
تنص سياسة الخصوصية على عدم تفعيل أي من ملفات تعريف الارتباط المستخدمة إلا بعد موافقة المستخدم، بحيث يكون الوضع الافتراضي هو عدم تفعيلها			36	23.5%	117	76.5%	0.12	6
تنص السياسة صراحة على حق المستخدم في الحماية من الاستغلال والإيذاء النفسي والجسدي والمعاملة المهنية			16	10.5%	137	89.5%	0.05	8
تحتوي سياسة الخصوصية على بند خاص بالخصوصية للأطفال	102	66.7%	8	5.2%	43	28.1%	0.69	2
المتوسط الحسابي العام	0.34							

من جدول (٣) يتضح أن التزام سياسات الخصوصية لتطبيقات الصحة المتنقلة عينة الدراسة فيما يتعلق بمحور القواعد والممارسات العامة جاء متوسطا إذ بلغ متوسطه الحسابي (٠,٣٤). وبتحليل بيانات الجدول يتضح أن:

- أكثر البنود التي حرص مطورو التطبيقات على توافرها في سياسات الخصوصية هو" هناك وسيلة للتواصل بين المستخدم ومقدم الخدمة للرد على التساؤلات الخاصة بحماية الخصوصية" فقد توافر هذا البند في(٨٣٪) من سياسات الخصوصية عينة الدراسة وقد تمثلت وسيلة التواصل في البريد الالكتروني لمطوري التطبيق مما يعطي الفرصة لمستخدمي التطبيقات بالاستفسار حول قضايا الخصوصية أثناء استخدامهم للتطبيق، بينما لم يقدم (٢٦) تطبيق بنسبة (١٧٪) أي وسيلة للتواصل مع المستخدم.
- جاء بند " تحتوي سياسة الخصوصية على بند خاص بالخصوصية للأطفال" في المرتبة الثانية حيث اهتمت غالبية التطبيقات بنسبة (٦٦,٧٪) بتوافر بند خاص بالخصوصية للأطفال، فوفقا لما جاء في سياسة الخصوصية لـ (١٠٢) تطبيق [في حالة اكتشافنا أن فردًا دون سن ١٣ قد زودنا بمعلومات شخصية دون موافقة الوالدين، فسنقوم على الفور بحذف البيانات وإلغاء تنشيط حساب الفرد]، بينما اهتمت (٨) تطبيقات بنسبة (٥,٢٪) بهذا البند جزئيا حيث اكتفت بكتابة ما يلي [أنت تتعهد بأنك قد قرات وفهمت ووافقت على سياسة الخصوصية وأن عمرك يزيد عن ١٦ عاما] بينما جاء في البعض الآخر ما يلي[نوصي القاصرين بتشجيع والديهم أو أولياء أمورهم على قراءة سياسة الخصوصية هذه وننصح القاصرين بالسعي للحصول على موافقة الوالدين أو الوصي والتوجيه قبل تقديم المعلومات الشخصية]والبعض ذكر[يُرجى عدم استخدام خدماتنا إذا كان عمرك أقل من ١٣ عاما] كل ذلك دون أن تذكر أنها ستقوم بحذف البيانات إذا ما تم إبلاغها بأن المستخدم يقل عمره عن ١٣ أو ١٦ عاما، وهذا يدل على أن تلك التطبيقات تحاول إخلاء

مسؤوليتها تجاه خصوصية الأطفال وتلقي بالمسؤولية كاملة على عاتق أولياء الأمور دون أن تُقدم لهم حلولا في حالة استخدام الطفل للتطبيق دون موافقة ولي الأمر، كما تجاهل (٤٣) تطبيق بنسبة (٢٨,١٪) خصوصية الأطفال ولم تعالج قضايا الخصوصية المتعلقة بهم على الإطلاق وبذلك فهي لم تراع قوانين حماية خصوصية الأطفال على الانترنت.

- وفي المرتبة الثالثة يأتي بند " تتسم نصوص سياسة الخصوصية بالوضوح وسهولة الفهم من قبل المستخدم" حيث اتسمت سياسات الخصوصية لـ (٣٥) تطبيق بنسبة (٢٢,٩٪) فقط بالاختصار والشفافية، حيث كُتبت بلغة مباشرة وواضحة، بينما انطبق جزئيا على (٤٠) تطبيق بنسبة (٢٦,١٪)، بينما فشل مطوري (٧٨) تطبيق بنسبة (٥١٪) في تقديم المعلومات بطريقة واضحة مما يجعلها غير قابلة للفهم من قبل المستخدم العادي، فقد لاحظت الباحثة أن الكثير من سياسات الخصوصية التي تم تحليلها طويلة بشكل مُبالغ فيه، وتُخفى المعلومات في روابط وصفحات متعددة، مما قد يصيب المستخدم بالملل والرغبة في عدم الاستمرار في القراءة، كما وجدت البعض منها موجزة ومختصرة بشدة فهي تُقدم معلومات شحيحة للمستخدمين مما يخل بالهدف منها، ومما يزيد الأمر صعوبة أن غالبيتها متاحة باللغة الإنجليزية وبذلك فهي لا تحتاج فقط إلى مستوى عال من التعليم حتى يتمكن المستخدم من قراءتها وفهمها، ولكن تحتاج أيضا إلى معرفة خاصة بالمصطلحات التقنية والقانونية المتخصصة.

- في المرتبة الرابعة جاء بند" تنص سياسة الخصوصية على تمكين المستخدم من خيارات رفض أو قبول استخدام ملفات تعريف الارتباط في التطبيق" حيث حرص (١٠٤) تطبيق على هذا البند جزئيا بنسبة (٦٨٪) فقد جاء في بيان الخصوصية لتلك التطبيقات ما يلي[لديك خيار إما قبول أو رفض ملفات تعريف الارتباط. إذا اخترت رفض ملفات تعريف الارتباط الخاصة بنا، فقد لا تتمكن من استخدام بعض أجزاء أو وظائف هذه الخدمة] فهي أعطت الحرية للمستخدم في حظر ملفات تعريف الارتباط عن طريق إيقاف عملها من إعدادات المتصفح الخاص به دون أن توضح له طريقة عمل ذلك، وفي نفس الوقت قيدت هذه الحرية عندما ذكرت أن استخدامه لخدمات ووظائف التطبيق قد تتأثر نتيجة لرفضها، ومن المعروف أن هذه الملفات تمثل انتهاكا صارخا لخصوصية المستخدم فهي من الوسائل المستخدمة لتتبع استخدام التطبيق وتجميع معلومات عن المستخدمين، بينما تجاهل (٤٩) تطبيق بنسبة (٣٢٪) هذا البند تماما.

- تلا ذلك في المرتبة الخامسة بند" تتضمن سياسة الخصوصية تعريفات واضحة وغير قابلة للتأويل لجميع المصطلحات القانونية والتقنية المستخدمة في بنود الخصوصية" فقد حرص (٢٢) تطبيق فقط بنسبة (١٤,٤٪) على تعريف المصطلحات المستخدمة في السياسة مثل (البيانات الشخصية، بيانات الاستخدام، مُقدم الخدمة، مُعالج البيانات، مُراقب البيانات، الأطراف الثالثة، ملفات تعريف الارتباط، تقنيات التتبع) وهو ما يساعد المستخدم على فهم بنود سياسة الخصوصية، كما اهتم بهذا البند جزئيا (١٥) تطبيق بنسبة (٩,٨٪) حيث اكتفت بتعريف مصطلحين أو ثلاثة على الأكثرتمثل أغلبها في (البيانات الشخصية، ملفات تعريف الارتباط)، في حين أهمل (١١٦) تطبيق بنسبة (٧٥,٨٪) هذا البند نهائيا، وهو ما يجعل سياسات الخصوصية غير واضحة وغير مفهومة لكثير من المستخدمين .

- وفي المرتبة السادسة جاء البند" تنص سياسة الخصوصية على عدم تفعيل أي من ملفات تعريف الارتباط المستخدمة إلا بعد موافقة المستخدم، بحيث يكون الوضع الافتراضي هو عدم تفعيلها" حيث ورد هذا البند جزئيا في (٣٦) تطبيق بنسبة (٢٣,٥٪) حيث جعلت شرط الموافقة الصريحة ملزما على أنواع معينة من ملفات تعريف الارتباط أما الأنواع الأخرى فهي إلزامية ويتم تفعيلها

بشكل افتراضي فلا تحتاج لموافقة المستخدم حيث جاء في بيان الخصوصية لتلك التطبيقات ما يلي[تم تصنيف ملفات تعريف الارتباط من حيث الوظيفة إلى ثلاث أنواع (ضرورية، إحصائية، المفضلة) يطلب التطبيق الموافقة على المفضلة والإحصائية من خلال اشعار، أما ملفات تعريف الارتباط الضرورية فلا يمكن للموقع أن يعمل بشكل صحيح بدونها، لا تحتاج إلى موافقة المستخدم] كما ورد في بعض السياسات ما يلي[سنطلب موافقتك لوضع ملفات تعريف الارتباط على جهازك باستثناء الحالات التي تكون فيها ضرورية]، كما تجاهل (١١٧) تطبيق بنسبة (٧٦,٥٪) هذا البند نهائيا وهو ما يسبب الكثير من القلق لأنه يتتبع البيانات ويخزنها دون إذن أو علم صريح من المستخدم، وهو مخالفة صريحة للقوانين فقد أكدت اللائحة العامة لحماية البيانات(GDPR) على ضرورة أن يعطى المستخدم موافقته الصريحة قبل تخزين ملفات تعريف الارتباط على أجهزته أو غيرها من تقنيات التتبع **(مكاوي، ٢٠٢٢)**.

- أما بالنسبة لبند" سياسة الخصوصية متاحة بأكثر من لغة من ضمنها اللغة العربية" فلم ينطبق سوى على (١٦) تطبيق فقط بنسبة (١٠,٥٪)، أما غالبية التطبيقات بنسبة (٨٩,٥٪) فهي غير متاحة باللغة العربية مما يجعل هناك صعوبة في قراءتها وفهمها كما سبق الذكر.
- وأخيرا يأتي في المرتبة الأخيرة بند" تنص السياسة صراحة على حق المستخدم في الخصوصية والحماية من الاستغلال والإيذاء النفسي والجسدي والمعاملة المهنية" فقد توافر هذا البند جزئيا في (١٦) تطبيق بنسبة (١٠,٥٪) فقط متمثلا في بعض العبارات مثل [نحن نحترم حقوق الخصوصية للمستخدم ونقر بأهمية حماية المعلومات التي تم جمعها عنه] أو [تتعهد الشركة باحترام سرية بياناتك الشخصية وضمان قدرتك على ممارسة حقوقك القانونية]، بينما تجاهله تماما (١٣٧) تطبيق بنسبة (٨٩,٥٪).

ثانيا: جمع البيانات :

إن جمع البيانات بدون معرفة المستخدم يعتبر جريمة يعاقب عليها القانون، لذا لابد أن يذكر مطورو تطبيقات الصحة المتنقلة في سياسة الخصوصية للتطبيق بمنتهى الوضوح والدقة نوعية البيانات والمعلومات التي يتم جمعها سواء التي تُطلب من المستخدم بشكل مباشر، أو تلك التي يتم جمعها بواسطة برمجيات معينة يستخدمها مقدم الخدمة كملفات تعريف الارتباط وعلامات البكسل ومعرفات الأجهزة المحمولة وغيرها من التقنيات المماثلة. ويذكر **المعداوي(٢٠١٨)** أن القانون يشترط ضرورة الحصول على موافقة المستخدم الصريحة والمسبقة قبل استخدام ومعالجة بياناته الشخصية والحساسة، ومن المعروف أن أنواع البيانات المختلفة تتطلب مستويات متباينة ومختلفة من الخصوصية. ويوضح جدول رقم (٤) مدى التزام مطورو تطبيقات الصحة المتنقلة عينة الدراسة بالكشف عن ممارساتهم فيما يتعلق بجمع البيانات من المستخدم ونوعيتها.

جدول رقم (٤): مستوى امتثال تطبيقات الصحة المتنقلة عينة الدراسة لأفضل ممارسات جمع البيانات من المستخدمين

البنود	نعم		جزئيا		لا		المتوسط الحسابي	الترتيب
	ت	النسبة٪	ت	النسبة٪	ت	النسبة٪		
توضح سياسة الخصوصية طريقة جمع البيانات بطريقة لا لبس فيها أو غموض.	126	82.4%			27	17.6%	0.82	1
تنص سياسة الخصوصية على طلب الموافقة الصريحة لبدء تخزين وجمع بيانات صحة المستخدم والبيانات الحساسة عند إنشاء الحساب	44	28.8%	16	10.5%	93	60.8%	0.34	3
تحتوي بنود سياسة الخصوصية على قائمة كاملة بالبيانات التي تجمعها ملفات تعريف الارتباط	46	30.1%	38	24.8%	69	45.1%	0.42	2
تنص سياسة الخصوصية على مدة الاحتفاظ بهذه بالبيانات التي تجمعها ملفات تعريف الارتباط	7	4.6%	11	7.2%	135	88.2%	0.08	4
تنص سياسة الخصوصية بوضوح تأثير رفض المستخدم تقديم البيانات الشخصية التي يطلبها التطبيق.			4	2.6%	149	97.4%	0.01	5
المتوسط الحسابي العام	0.34							

حيث يتبين من جدول رقم (٤) أن التزام مقدمو الخدمة لتطبيقات الصحة المتنقلة عينة الدراسة بالكشف عن ممارسات جمع البيانات من المستخدمين كان متوسطا حيث بلغ المتوسط الحسابي لهذا المحور (٠,٣٤)، مما يعني أن سياسات الخصوصية لتلك التطبيقات لم تتحلى بعنصر الشفافية بالقدر الكاف فيما يخص ما هي البيانات التي تجمعها وطريقة استخدامها، ومن تحليل بيانات الجدول يتبين ما يلي:

- أن بند" توضح سياسة الخصوصية طريقة جمع البيانات بطريقة لا لبس فيها أو غموض " جاء في المرتبة الأولى، حيث التزم (١٢٦) تطبيق بنسبة (٨٢,٤٪) بالكشف عن طرق جمعهم للبيانات، فقد ذكرت تلك التطبيقات أن هناك بيانات شخصية تطلبها من المستخدم مباشرة مثل(الاسم، البريد الالكتروني، تاريخ الميلاد، البيانات الصحية كالوزن والطول، ضغط الدم، اللياقة البدنية وغيرها)، وهناك بيانات غير شخصية يتم جمعها تلقائيا باستخدام ملفات تعريف الارتباط وبرمجيات تحليل الويب مثل (بروتكول الانترنت للجهاز IP، ونوع الجهاز، ونوع المتصفح، الموقع الجغرافي، وبيانات الاستخدام للتطبيق وغيرها) وهناك بيانات يتم جمعها من مواقع التواصل الاجتماعي إذا قرر المستخدم التسجيل في التطبيق باستخدام حساب فيسبوك مثلا، بينما جاءت طرق جمع البيانات غير واضحة وغامضة في (٢٧) تطبيق بنسبة (١٧,٦٪) حيث اكتفت تلك التطبيقات بعبارات مبهمة ومقتضبة مثل (يجوز لنا جمع معلومات عنك وعن أجهزتك واستخدامك للتطبيق بالطرق التي قد نوضحها لك وقت الجمع).
- في المرتبة الثانية جاء بند" تحتوي بنود سياسة الخصوصية على قائمة كاملة بالبيانات التي تجمعها ملفات تعريف الارتباط"، حيث التزم (٤٦) تطبيق بنسبة (٣٠,١٪) بإعلام المستخدم بأنواع البيانات التي تجمعها ملفات تعريف الارتباط بشئ من التفصيل حيث قسمتها إلى بيانات فنية مثل (نوع المتصفح وإصداره، بروتكول الانترنت، اللغة المفضلة، الموقع الجغرافي، معرفات الجهاز،.....)، وبيانات الاستخدام للتطبيق مثل (تاريخ ووقت الزيارة، الصفحات التي تم زيارتها، مصطلحات البحث المستخدمة، عمليات الشراء والمعاملات المالية للمستخدم،.....)،

كما التزم (٣٨) تطبيق بنسبة (٢٤,٨٪) بهذا البند جزئيا حيث جاء في سياسات الخصوصية لتلك التطبيقات[نحن نجمع معلومات غير شخصية عنك بمساعدة أطراف ثالثة ومنها على سبيل المثال وليس الحصر .....]، بينما لم يفصح (٦٩) تطبيق بنسبة (٤٥,١٪) عن البيانات التي تجمعها ملفات تعريف الارتباط مطلقا، حيث اكتفت تلك التطبيقات بعبارات واسعة وفضفاضة مثل[نحن نستخدم أدوات تحليل تابعة لجهات خارجية لمساعدتنا في قياس اتجاهات حركة المرور والاستخدام للتطبيق] أو [يستخدم تطبيقنا بعض مقدمي الخدمة لعرض الإعلانات، يمكن لمقدمي الإعلانات استخدام ملفات تعريف الارتباط لتحديد جهازك وعرض الإعلانات ذات الصلة باهتماماتك].

- أما بند" تنص سياسة الخصوصية على طلب الموافقة الصريحة لبدء تخزين وجمع بيانات صحة المستخدم والبيانات الحساسة عند إنشاء الحساب" فقد جاء في المرتبة الثالثة، حيث التزم (٤٤) تطبيق فقط بنسبة (٢٨,٨٪) بطلب موافقة المستخدم الصريحة على جمع البيانات وذلك من خلال النقر الإيجابي للمربع للموافقة على بدء معالجة البيانات الصحية الشخصية حيث جاء بيان ذلك في سياسات الخصوصية [من خلال تحديد المربع، فإنك توافق على معالجة البيانات الصحية الشخصية التي تقدمها عند استخدام التطبيق] كما ورد أيضا[البيانات البيومترية هي فئة خاصة من البيانات الشخصية بموجب اللائحة العامة لحماية البيانات، والتي تُحظر افتراضيا باستثناء بعض الحالات بما في ذلك الموافقة الصريحة]، كما تحايل (١٦) تطبيق بنسبة (١٠,٥٪) على هذا الأمر حيث لم تطلب تلك التطبيقات موافقة المستخدم الصريحة بل اكتفت بعبارة [انشاء الحساب معناه الموافقة على جمع البيانات] فقد اعتمدت على أن المستخدم قام بقراءة سياسة الخصوصية قبل تثبيت التطبيق وإنشاء الحساب ومن ثم فهو موافق على جمع بياناته، بينما لم يتطرق (٩٣) تطبيق بنسبة (٦٠,٨٪) لهذا البند نهائيا، وهو ما يُعد انتهاكا صارخا للوائح وقوانين الخصوصية حيث تنص المادة (٢) من القانون المصري ١٥١ لسنة ٢٠٢٠ بضرورة موافقة الشخص المعني بالبيانات الشخصية موافقة صريحة حتى يكون التعامل في البيانات تعاملا مشروعا، وفيما يتعلق بالبيانات الشخصية الحساسة فقد نص المشرع في المادة (١٢) من نفس القانون على حظر التعامل في البيانات الحساسة إلا في حال الحصول على موافقة الشخص المعني بالبيانات موافقة كتابية صريحة، كما أنه بموجب اللائحة العامة لحماية البيانات فقد نصت المادة (٦) على أنه لا تكون المعالجة قانونية إلا إذا أعطى صاحب البيانات الموافقة على معالجة بياناته الشخصية لغرض واحد أو أكثر من الأغراض المحددة، بشرط أن يكون طلب الحصول على الموافقة واضح ومحدد وصريح في تحديد البيانات التي سيتم معالجتها وبلغة واضحة ومفهومة لا لبس فيها، و يجب أن يتخذ الشخص المعني بالبيانات إجراء إيجابيا واضحا كمؤشر لقبول معالجة البيانات الشخصية، بحيث لا يمكن اعتبار مجرد السكوت أو عدم الاعتراض دليلا على الموافقة(عبد الرحمن، ٢٠٢٢).
- أما المرتبة الرابعة فقد احتلها بند" تنص سياسة الخصوصية على مدة الاحتفاظ بهذه البيانات التي تجمعها ملفات تعريف الارتباط" فلم يلتزم سوى (٧) تطبيقات بنسبة (٤,٦٪) فقط ببيان عمر ملفات تعريف الارتباط المستخدمة، حيث أوضحت تلك التطبيقات أنها تستخدم ملفات تعريف الارتباط للجلسة والتي يتم إزالتها من الجهاز بمجرد إغلاق المتصفح، كما تستخدم ملفات تعريف الارتباط الدائمة والتي يتم الاحتفاظ بها لفترات مختلفة (شهر، سنة ، ٦ أشهر، سنتان)، بينما التزم (١١) تطبيق بنسبة (٧,٢٪) بهذا البند جزئيا، حيث جاء في سياسات الخصوصية لتلك التطبيقات [نستخدم ملفات تعريف الارتباط الثابتة والتي يمكن أن تظل على جهازك حتى انتهاء صلاحيتها والتي قد تصل في بعض الحالات ١٠ سنوات] فهي لم تُحدد فترات محددة لكل نوع من أنواع

ملفات تعريف الارتباط، في حين لم يلتزم (١٣٥) تطبيق بنسبة (٨٨,٢٪) بإيضاح ذلك للمستخدم. وهو ما يشكل مصدر قلق كبير لخصوصية المستخدم فملفات تعريف الارتباط الدائمة معروفة باسم ملفات تعريف الارتباط للتتبع حيث يمكن للمعلنين استخدامها لتسجيل معلومات حول عادات تصفح الويب للمستخدم على مدار فترات زمنية طويلة، ومعني ذلك أنه قد تظل تلك الملفات على جهاز المستخدم حتى بعد الغاء اشتراكه في التطبيق إلا إذا قام هو بحذفها بنفسه وهو ما يغفله الكثير من المستخدمين.

- وأخيرا في المرتبة الخامسة والأخيرة جاء بند " تنص سياسة الخصوصية بوضوح تأثير رفض المستخدم تقديم البيانات الشخصية التي يطلبها التطبيق" فقد التزم (٤) تطبيقات فقط بنسبة (٢,٦٪) بهذا البند جزئيا حيث قامت بإيضاح ذلك لكن بعبارات مختصرة للغاية فقد جاء على سبيل المثال في بيان الخصوصية لتلك التطبيقات [أنت لست ملزما بتقديم معلوماتك الشخصية، ولكن يرجى ملاحظة أن معظم وظائف التطبيق تعتمد على معلومات عنك وعن صحتك، وبدون تقديم هذه المعلومات قد لا تتمكن من استخدام الوظائف على الإطلاق، وفي بعض الحالات قد تتأثر دقة النتائج] كما جاء في أحد التطبيقات أن [هناك بيانات إلزامية والتي يستحيل بدونها تقديم الخدمة، كما أن هناك بيانات غير إلزامية يكون للمستخدم الحرية في عدم تقديمها دون عواقب على توفر الخدمة أو وظائفها]، بينما لم تتطرق سياسة الخصوصية لـ (١٤٩) تطبيق بنسبة (٩٧,٤٪) لهذا البند نهائيا.

وفيما يلي نستعرض نوعية البيانات التي تجمعها تطبيقات الصحة المتنقلة عينة الدراسة والأذونات التي تطلبها أيضا.

أ/ البيانات التي تجمعها تطبيقات الصحة المتنقلة عينة الدراسة:

جدول رقم (٥): أنواع البيانات التي تجمعها تطبيقات الصحة المتنقلة عينة الدراسة

البيانات التي يتم جمعها		ت	النسبة٪
بيانات شخصية تُطلب من المستخدم	الاسم	124	81.0%
	البريد الالكتروني	124	81.0%
	كلمة المرور	86	56.2%
	عنوان المنزل أو العمل(مكان الإقامة)	7	4.6%
	تاريخ الميلاد والعمر	77	50.3%
	نوع الجنس	81	52.9%
	أرقام الهاتف	62	40.5%
	الاهتمامات	4	2.6%
	المهنة	3	2.0%
	رقم بطاقة الهوية الشخصية	1	0.7%
	رقم جواز السفر	1	0.7%
	الحالة الاجتماعية	1	0.7%
بيانات شخصية حساسة تُطلب من المستخدم	بيانات حساسة للغاية	59	38.6%
	بيانات بيومترية	9	5.9%
	النشاط البدني	77	50.3%
	بيانات صحية(الوزن، الطول، درجة الحرارة،...)	73	47.7%
	بطاقة الائتمان	43	28.1%

بيانات فنية تُجمع تلقائيا	الموقع الجغرافي	74	48.4%
	عنوان بروتكول الانترنت للجهاز ip	98	64.1%
	نوع جهاز المحمول المستخدم	98	64.1%
	نوع متصفح الانترنت على جهاز المحمول	95	62.1%
	إصدار المتصفح	95	62.1%
	طريقة الاتصال بالانترنت	90	58.8%
	نظام التشغيل للهاتف المحمول	91	59.5%
	حجم الشاشة	22	14.4%
	اللغة المفضلة	87	56.9%
	حسابات مواقع التواصل الاجتماعي	38	24.8%
بيانات استخدام التطبيق تُجمع تلقائيا	عدد مرات الاستخدام	86	56.2%
	الاستجابة للعروض والإعلانات	84	54.9%
	وقت وتاريخ الزيارة	86	56.2%
	الصفحات التي تم زيارتها	86	56.2%

يكشف الجدول رقم (٥) عن نوعية البيانات التي تجمعها تطبيقات الصحة المتنقلة من مستخدميها، وذلك بناءً على ما تم الكشف عنه صراحةً في سياسات الخصوصية لتلك التطبيقات، وهذا يعني أنها قد تجمع بيانات أكثر من ذلك ولم يُصرح بها في سياسات الخصوصية حيث اكتفت غالبية التطبيقات بذكر البيانات على سبيل المثال وليس الحصر، وتتنوع هذه البيانات ما بين بيانات شخصية تُحدد هوية المستخدم، وبيانات شخصية حساسة، وبيانات غير شخصية لا تكشف عن هوية المستخدم، ويوضح الجدول التالي هذه البيانات ومعدل تكرار طلبها وفقا لما نصت عليه سياسات الخصوصية للتطبيقات عينة الدراسة، في محاولة للتأكد من معالجة البيانات الشخصية التي تحتاجها تلك النوعية من التطبيقات فعليا دون سواها من البيانات.

حيث يتضح من الجدول رقم (٥) أن تطبيقات الصحة المتنقلة عينة الدراسة تجمع بيانات تفصيلية عن المستخدمين وهو ما قد يمثل انتهاكا لحرمة الحياة الخاصة، فمثل هذه التطبيقات لا يمكن الانضمام إليها بدون إنشاء حساب شخصي وتقديم بيانات شخصية، والتي تتحول مع الوقت إلى كمية هائلة من المعلومات الشخصية والحساسة التي يتم معالجتها للتعرف على الأنماط السلوكية للمستخدم، ويمكن توضيح ذلك فيما يلي:

- أولا: فيما يتعلق بالبيانات الشخصية التي تطلبها التطبيقات عينة الدراسة من المستخدمين، فقد جاء على رأسها الاسم والبريد الالكتروني حيث تم طلبهما فيما نسبته (٨١٪) من التطبيقات، تلا ذلك كلمة المرور حيث تم ذكرها في (٥٦,٢٪) من التطبيقات، ونوع الجنس في (٥٢,٩٪) من التطبيقات، ثم تاريخ الميلاد في نسبة (٥٠,٣٪)، وأرقام الهاتف في (٤٠,٥٪) من التطبيقات، وكل هذه البيانات ترى الباحثة أنه من الطبيعي بل والضروري أن تطلبها تلك التطبيقات حتى تستطيع أداء المهام الموكلة بها وتقديم خدماتها والتواصل مع المستخدمين، ولكن الأمر المحير هو بعض البيانات التي ورد ذكرها في عدد ضئيل جدا من التطبيقات كعنوان المنزل أو العمل، المهنة، الاهتمامات، والأغرب من ذلك رقم بطاقة الهوية الشخصية، ورقم جواز السفر والحالة الاجتماعية والتي ورد ذكرها في تطبيق واحد فقط، وترى الباحثة أن هذه النوعية من البيانات تتجاوز الغرض الأساسي المحدد الذي تُجمع البيانات من أجله وهو تقديم خدمات الرعاية الصحية وتحسين الصحة العامة للمستخدمين، وهو ما يُعد تجاوزا لمبدأ أساسي من المبادئ الرئيسية

لخصوصية البيانات وهو تقليل البيانات، ويبقى السؤال هنا هل هناك تطبيقات أخرى تطلب تلك النوعية من البيانات دون أن تذكر ذلك في سياسة الخصوصية؟

- ثانيا: فيما يخص البيانات الشخصية الحساسة التي تطلبها التطبيقات عينة الدراسة من المستخدمين وفقا للتعريف الإجرائي لها في هذه الدراسة، فيأتي على رأسها بيانات النشاط البدني والتي ورد ذكرها في نسبة (٥٠,٣٪) من التطبيقات، تلا ذلك البيانات الصحية (كالوزن، الطول، درجة الحرارة،...) والتي ورد ذكرها فيما نسبته (٤٧,٧٪)، ثم نوعية من البيانات رأت الباحثة أنها حساسة للغاية والتي ورد ذكرها في (٣٨,٦٪) من التطبيقات، كما ورد ذكر بيانات بطاقة الائتمان في (٢٨,١٪) من التطبيقات، وأخيرا البيانات البيومترية[٣] (كبصمة الإصبع وصورة الوجه) والتي ورد ذكرها في (٩) تطبيقات بنسبة (٥,٩٪)، بذلك فهي تجمع قدرا كبيرا من البيانات الحساسة عن المستخدمين، وهو ما يُعرض خصوصية المستخدم للخطر وخاصة إذا ما تم مشاركتها مع أطراف ثالثة دون موافقة صريحة من المستخدم.
- ثالثا: بالنسبة للبيانات الفنية التي تُجمع تلقائيا من خلال ملفات تعريف الارتباط وعلامات البكسل وغيرها من تقنيات التتبع، يأتي على رأسها عنوان بروتكول الانترنت للجهاز IP ونوع جهاز المحمول المستخدم واللذان ورد ذكرهما في (٦٤,١٪) من التطبيقات، وبالنسبة لعنوان ال IP رغم أن جميع التطبيقات ذكرته على أساس أنه نوع من البيانات غير الشخصية، إلا أن الباحثة ترى أنه ينبغي إدراجه من ضمن البيانات الشخصية للمستخدم، فهو يحدد الصفحات التي قام المستخدم بزيارتها وتاريخ ووقت الاتصال، وهذا من شأنه أن يكشف عن ميول واتجاهات المستخدمين، ويحدد أماكن اتصالهم بالإنترنت، بل قد يحدد عاداتهم اليومية ومواعيد العمل من خلال تحديد ساعات الاتصال بالهاتف، وغير ذلك الكثير، تلا ذلك نوع المتصفح وإصدار المتصفح حيث ورد ذكرهما في نسبة (٦٢,١٪) من التطبيقات، كما ورد ذكر نظام التشغيل للهاتف في (٥٩,٥٪) من التطبيقات، كما ذكر (٧٤) تطبيق بنسبة (٤٨,٤٪) أنه يجمع بيانات عن الموقع الجغرافي، وذكر (٣٨) تطبيق بنسبة (٢٤,٨٪) أنه يجمع بيانات عن حسابات مواقع التواصل الاجتماعي، أما حجم الشاشة فقد ورد ذكره في (٢٢) تطبيق بنسبة (١٤,٤٪)، والجدير بالذكر أن تلك النوعيات من البيانات التي تجمعها ملفات تعريف الارتباط هي في الحقيقة تابعة لجهات خارجية مما يشكل تهديداً خطيراً للخصوصية، فهذه الجهات هدفها الأول هو جمع أكبر قدر من المعلومات عن المستخدم لتحديد هويته وتتبعه لتزويده بإعلانات مستهدفة وفقا لاهتماماته و سلوك التصفح الخاص به، إذا فهي تحقق أرباحا من بيانات المستخدم الخاصة عن طريق بيعها لشركات الإعلانات.
- رابعا: بيانات استخدام التطبيق: وهي بيانات تُجمع تلقائيا الغرض الأساسي منها هو مراقبة أداء التطبيق وذلك للحفاظ على مستوى الخدمة وتحسينها، مثل عدد مرات استخدام التطبيق والصفحات التي تم زيارتها وتاريخ ووقت الزيارة والتي ورد ذكرها صراحة في (٨٦) تطبيق بنسبة (٥٦,٢٪)، وكذلك معلومات عن الاستجابة للعروض والإعلانات والتي ورد ذكرها في (٨٤) تطبيق بنسبة (٥٤,٩٪)، والمشكلة في هذا النوع من البيانات أن التطبيقات تشارك بيانات المستخدم مع جهات خارجية لمراقبة وتحليل استخدام خدماتها، وهي في حقيقة الأمر تستخدم بيانات المستخدمين لأغراض أخرى كبيعها للمنصات الإعلانية، وخاصة وأنها تطبيقات مجانية ومن ثم فبيع معلومات المستخدمين لأطراف ثالثة هو مصدر ربحها.

ب/ الأذونات التي تطلبها تطبيقات الصحة المتنقلة عينة الدراسة:

حتى يتمكن المستخدم من تثبيت التطبيق على جهازه المحمول أو لاستخدام وظيفة معينة من وظائف التطبيق، يُطلب منه في كثير من الأحيان أن يمنح الإذن للتطبيق للوصول إلى بيانات الهاتف المحمول للمستخدم، وتعديل أو إضافة أو إزالة بيانات، والتحكم أيضا في أجزاء الهاتف المختلفة كالكاميرا أو الميكروفون، ويعرض الجدول رقم (٦) بعض أنواع الأذونات Permissions التي تطلبها تطبيقات الصحة المتنقلة عينة الدراسة، والتي ترى الباحثة أنها الأكثر خطورة، سواء التي تم ذكرها صراحة في سياسات الخصوصية، أو تلك التي يوفرها متجر جوجل بلاي كمعلومات عن التطبيق، وبالنظر إلى أنواع الأذونات المطلوبة يتبين سعى تلك التطبيقات إلى الوصول لأكبر قدر ممكن من بيانات المستخدم، بصرف النظر عن إذا ما كانت مطلوبة لأداء وظائف التطبيقات أم لا.

جدول رقم (٦): أنواع الأذونات التي تطلبها تطبيقات الصحة المتنقلة عينة الدراسة

الأذونات التي تطلبها التطبيقات	ت	النسبة٪
إذن المعرف الإعلاني	124	81.0%
عرض اتصالات Wi-Fi	124	81.0%
مساحة التخزين	103	67.3%
الكاميرا	55	35.9%
الموقع	43	28.1%
الهاتف	33	21.6%
جهات الاتصال	23	15.0%
الميكرفون	19	12.4%
إعدادات البلوتوث	18	11.8%
استخدام الأجهزة البيومترية	17	11.1%
التقويم	15	9.8%
الرسائل القصيرة	12	7.8%
إعدادات الصوت	11	7.2%
سجل المكالمات	10	6.5%
أجهزة استشعار الجسم	8	5.2%

يتبين من الجدول أن تطبيقات الصحة المتنقلة تطلب عدد كبير من الأذونات، والتي قد تستغلها في جمع بيانات المستخدمين لأغراض غير معلنة تجارية واستثمارية، مستغلة في ذلك جهل المستخدمين بأمر هذه الاذونات.

حيث طلب (١٢٤) تطبيق بنسبة (٨١٪) إذن المعرف الإعلاني وعرض اتصالات Wi-Fi، والمعرف الإعلاني هو معرف فريد على أجهزة الأندرويد وظيفته الأساسية هي الدعاية، حيث يستخدم من أجل تتبع وبيع نشاط المستخدم لعرض الإعلانات الموجهة عليه، فهو يعمل بطريقة تشبه ملفات تعريف الارتباط، كما أن هناك (١٠٣) تطبيق بنسبة (٦٧,٣٪) تطلب إذن الوصول إلى مساحة التخزين، مما يمنحها القدرة على الوصول إلى كل الملفات الموجودة على هاتف المستخدم بأنواعها المختلفة مثل مقاطع الفيديو والصور والملفات الصوتية ويسمح للتطبيق بإمكانية تعديلها أو حذفها، وهو ما يمكن استغلاله في الدخول

إلى ذاكرة تخزين الهاتف و الوصول إلى ملفات تعريف الارتباط لتتبع ومعرفة ما يبحث عنه المستخدم على الانترنت.

كما يطلب (٥٥) تطبيق بنسبة (٣٥,٩٪) إذن الوصول إلى الكاميرا، وطلب (٤٣) تطبيق بنسبة (٢٨,١٪) إذن الوصول إلى الموقع الجغرافي، مما يسمح للتطبيق بتحديد موقع المستخدم طالما كان متصلا بالإنترنت، وهناك (٣٣) تطبيق بنسبة (٢١,٦٪) طلب إذن الوصول إلى الهاتف، مما يسمح للتطبيق بالوصول إلى رقم هاتف المستخدم ومعلومات الشبكة، ويطلب (٢٣) تطبيق بنسبة (١٥٪) إذن الوصول إلى جهات الاتصال والأرقام المسجلة على الهاتف، كما طلب (١٩) تطبيق بنسبة (١٢,٤٪) إذن الوصول للميكرفون، وهناك (١٨) تطبيق بنسبة (١١,٨٪) طلبت إذن الوصول إلى إعدادات البلوتوث، وطلب (١٧) تطبيق بنسبة (١١,١٪) إذن الوصول إلى الأجهزة البيومترية، في حين طلب (١٥) تطبيق بنسبة (٩,٨٪) إذن الوصول إلى التقويم ومن ثم يكون للتطبيق القدرة على قراءة الأحداث والمواعيد المسجلة على هاتف المستخدم. كما طلب (١٢) تطبيق بنسبة (٧,٨٪) إذن الوصول إلى الرسائل القصيرة، ويطلب (١١) تطبيق بنسبة (٧,٢٪) إذن الوصول إلى إعدادات الصوت، وطلبت (١٠) تطبيقات بنسبة (٦,٥٪) إذن الوصول إلى سجل المكالمات، كما طلبت (٨) تطبيقات بنسبة (٥,٢٪) إذن الوصول لأجهزة استشعار الجسم كالساعات الذكية وذلك لمراقبة بيانات المستخدم الصحية كضربات القلب والضغط وتتبع اللياقة البدنية.

ونستنتج من تحليل الأذونات التي طلبتها التطبيقات عينة الدراسة أن هناك أذونات ضرورية وقد تحتاج إليها التطبيقات بالفعل لأداء مهمتها، ولكن هناك أيضا أذونات غير ضرورية وغير مبررة، فتطبيق طبي أو صحي لماذا يحتاج إذن الموصول للموقع الجغرافي وسجل المكالمات وجهات الاتصال، مما يؤكد أن هذه التطبيقات تستخدم الأذونات في أغراض أخرى.

ثالثا: أغراض جمع وتحليل البيانات:

تنص القوانين أنه يمنع على أي شخص أن يقوم بجمع أي بيانات شخصية يكون من شأنها تحديد هوية شخص معين، إلا إذا كان جمع هذه البيانات من أجل تحقيق أغراض مشروعة ومحددة وواضحة بعد الحصول على إذن وموافقة الشخص المراد الحصول على بياناته الشخصية **(المعداوي، ٢٠١٨)**، ويكشف جدول (٧) مدى التزام سياسات الخصوصية لتطبيقات الصحة المتنقلة عينة الدراسة بالكشف عن ممارساتها فيما يتعلق بأغراض جمع وتحليل البيانات.

جدول رقم (٧): مستوى امتثال تطبيقات الصحة المتنقلة عينة الدراسة لأفضل ممارسات أغراض جمع وتحليل البيانات

البنود	نعم		جزئيا		لا		المتوسط الحسابي	الترتيب
	ت	النسبة٪	ت	النسبة٪	ت	النسبة٪		
تشرح سياسة الخصوصية بشكل شفاف كيفية معالجة البيانات.	50	32.7%	52	34.0%	51	33.3%	0.50	2
تنص سياسة الخصوصية صراحة أن ليس من حق مقدم الخدمة أن يستخدم البيانات التي تم جمعها في أي غرض غير منصوص عليه في سياسة الخصوصية.	33	21.6%			120	78.4%	0.22	4
تنص بنود سياسة الخصوصية بوضوح على أغراض جمع البيانات التي يقدمها المستخدم بنفسه.	84	54.9%	36	23.5%	33	21.6%	0.67	1
تنص بنود سياسة الخصوصية بوضوح على أغراض جمع البيانات التي يجمعها التطبيق بواسطة ملفات تعريف الارتباط.	43	28.1%	26	17.0%	84	54.9%	0.37	3
المتوسط الحسابي العام	0.44							

حيث يتبين من الجدول رقم (٧) أن التزام مطورو تطبيقات الصحة المتنقلة عينة الدراسة بالكشف عن ممارساتهم فيما يتعلق بأغراض جمع وتحليل ومعالجة البيانات جاء متوسطا بمتوسط حسابي بلغ (٠,٤٤)، وبالنظر إلى الجدول السابق يتبين أن:

- احتل بند" تنص بنود سياسة الخصوصية بوضوح على أغراض جمع البيانات التي يقدمها المستخدم بنفسه" المرتبة الأولى حيث التزم (٨٤) تطبيق بنسبة (٥٤,٩٪) بإعلام المستخدم بالغرض من جمع البيانات الشخصية والصحية التي يطلبها التطبيق من المستخدم، بينما كشف (٣٦) تطبيق بنسبة (٢٣,٥٪) عن هذه الأغراض ولكن بصورة عامة وغير محددة مثل (لتقديم خدماتنا و التواصل مع المستخدمين وإدارة حسابك وتزويدك بالأخبار والعروض العامة) وهو ما يمثل خطرا على خصوصية المستخدمين حيث قد يستخدم مقدمو الخدمة بيانات المستخدمين بشكل يهدد خصوصيتهم دون انتهاك سياسات الخصوصية التي قاموا بوضعها، في حين لم يمتثل (٣٣) تطبيق بنسبة (٢١,٦٪) للوائح وقوانين الخصوصية في الكشف بوضوح عن أغراض جمع البيانات حيث لم يكشفوا في سياساتهم عن تلك الأغراض نهائيا، وبذلك تفتقد لمبدأ الشفافية، فوفقا للائحة العامة لحماية البيانات يجب أن تستند معالجة البيانات الشخصية دائما إلى غرض محدد، ووفقا للمادة (٣) من القانون ١٥١ لسنة ٢٠٢٠ يشترط لمعالجة البيانات الشخصية توافر مجموعة من الشروط منها أن تُجمع البيانات لأغراض مشروعة ومحددة ومعلنة للشخص المعني.
- وجاء بند" تشرح سياسة الخصوصية بشكل شفاف كيفية معالجة البيانات" في المرتبة الثانية، حيث جاءت طريقة معالجة البيانات واضحة في (٥٠) تطبيق بنسبة (٣٢,٧٪) حيث عرضت تلك التطبيقات الإجراءات التي تُجرى على البيانات الشخصية التي يتم جمعها من جمع وتخزين واستخدام ومشاركة مع جهات خارجية ونقل وتخزين وفي أي دولة تتم معالجة البيانات، بينما جاءت طريقة معالجة البيانات واضحة إلى حد ما في (٥٢) تطبيق بنسبة (٣٤٪)، في حين لم يلتزم (٥١) تطبيق بنسبة (٣٣,٣٪) بالكشف عن ممارساتهم في معالجة بيانات المستخدم.
- وفي المرتبة الثالثة جاء بند" تنص بنود سياسة الخصوصية بوضوح على أغراض جمع البيانات التي يجمعها التطبيق بواسطة ملفات تعريف الارتباط" حيث حرص (٤٣) تطبيق بنسبة (٢٨,١٪) على توضيح ذلك بالتفصيل، بينما عرض (٢٦) تطبيق بنسبة (١٧٪) أغراض جمع البيانات التي تجمعها ملفات تعريف الارتباط ولكن بطريقة مختصرة وعامة مثل (تحليل البيانات وتحديد اتجاهات الاستخدام وتقييم وتحسين خدماتنا ومنتجاتنا)، كما لم يُفصح (٨٤) تطبيق بنسبة (٥٤,٩٪) عن هذه الأغراض نهائيا.
- وفي المرتبة الرابعة والأخيرة جاء بند" تنص سياسة الخصوصية صراحة أنه ليس من حق مقدم الخدمة أن يستخدم البيانات التي تم جمعها في أي غرض غير منصوص عليه في سياسة الخصوصية" حيث التزم (٣٣) تطبيق بنسبة (٢١,٦٪) فقط بالتصريح بذلك حيث صرحت تلك التطبيقات أنها لن تستخدم البيانات التي تم جمعها لأي غرض آخر غير منصوص عليه في سياسة الخصوصية، كما صرح بعض منها أنها إذا أرادت استخدام المعلومات لأغراض أخرى لا تغطيها السياسة فسوف تحصل على موافقة المستخدم المسبقة، بينما أغفل وتجاهل (١٢٠) تطبيق بنسبة (٧٨,٤٪) التصريح بذلك تماما، وهنا يتبادر إلى الذهن سؤال مهم هل يحق للمستخدم مقاضاة مقدمو الخدمة والمطالبة بتعويض جراء انتهاك خصوصيته في حال تم استخدام بياناته لأغراض أخرى غير منصوص عليها في سياسة الخصوصية دون موافقته طالما أنهم لم يصرحوا في سياسة الخصوصية بأنهم لن يستخدموا البيانات لأغراض أخرى؟ فوفقا للائحة

العامة لحماية البيانات يجب عدم معالجة البيانات الشخصية لأغراض بخلاف ما وافق عليه المستخدم.

رابعا: مشاركة البيانات مع أطراف ثالثة:

عادة ما تقوم التطبيقات والمواقع بمشاركة البيانات التي تجمعها من المستخدمين مع جهات خارجية وأطراف ثالثة وذلك لأسباب مختلفة كتحليل بيانات المستخدم أو عرض الإعلانات القائمة على اهتماماته، مما يسهم في استمرارية التطبيق وخاصة المجانية منها، وغير ذلك. ومن ثم لابد أن يضمن مطورو التطبيق أن هذه الأطراف تطبق بالفعل ضوابط مناسبة لخصوصية البيانات الشخصية، مع إبلاغ المستخدم بدور كل طرف والتزاماته ومسؤولياته، وهنا لابد أن يلتزم مقدمو الخدمة لتطبيقات الصحة المتنقلة بالكشف عن ممارساتهم حيال ذلك في سياسات الخصوصية بطريقة شفافة وواضحة، وذلك ما يكشف عنه جدول رقم (٨).

جدول رقم (٨): مستوى امتثال تطبيقات الصحة المتنقلة عينة الدراسة لأفضل ممارسات مشاركة البيانات مع أطراف ثالثة

البنود	نعم		جزئيا		لا		المتوسط الحسابي	الترتيب
	ت	النسبة٪	ت	النسبة٪	ت	النسبة٪		
تنص سياسة الخصوصية بوضوح إذا كان التطبيق يشارك بيانات المستخدمين مع طرف ثالث.	134	87.6%			19	12.4%	0.88	1
تتسم بنود سياسة الخصوصية بالوضوح والشفافية في صياغة أحكام مشاركة البيانات مع أطراف ثالثة.	34	22.2%	49	32.0%	70	45.8%	0.38	5
تنص سياسة الخصوصية بوضوح على أسباب مشاركة البيانات مع أطراف ثالثة	68	44.4%	53	34.6%	32	20.9%	0.62	3
تنص سياسة الخصوصية على أن مشاركة البيانات مع أطراف ثالثة تستند على موافقة مسبقة من المستخدم.			24	15.7%	129	84.3%	0.08	7
تحدد سياسة الخصوصية بوضوح الأطراف الثالثة بشكل حصري.	64	41.8%	28	18.3%	61	39.9%	0.51	4
تنص سياسة الخصوصية على التزم مقدم الخدمة بعدم الإفصاح عن أي من البيانات والمعلومات الخاصة بالمستخدم لأي من جهات تنفيذ القانون إلا في حالة وجود أمر قضائي مسبق.	49	32.0%			104	68.0%	0.32	6
تنص سياسة الخصوصية بوضوح وبشكل حصري على برمجيات تحليل الويب التي يستخدمها التطبيق للتتبع والتحليل	106	69.3%			47	30.7%	0.69	2
تنص سياسة الخصوصية على التزم مقدمو الخدمة بعدم نقل البيانات الشخصية للمستخدم التي تم جمعها ومعالجتها إلى دولة أخرى إلا بعد الموافقة الصريحة من المستخدم.			12	7.8%	141	92.2%	0.04	8
المتوسط الحسابي العام	0.44							

فكما هو موضح في الجدول رقم (٨) جاء التزام مطورو تطبيقات الصحة المتنقلة عينة الدراسة بالكشف عن ممارساتهم فيما يتعلق بمشاركة بيانات المستخدمين مع أطراف ثالثة متوسطا بمتوسط حسابي بلغ (٠,٤٤)، ومعنى ذلك أن مقدمى الخدمة لتلك التطبيقات لم يتحلوا بالشفافية بالقدر الكاف فيما يخص

مشاركة البيانات، وقدموا معلومات شحيحة نوعا ما عن مرحلة مشاركة البيانات مع الأطراف الثالثة، ومن استقراء بيانات الجدول نجد أن :

- جاء بند" تنص سياسة الخصوصية بوضوح إذا كان التطبيق يشارك بيانات المستخدمين مع أطراف ثالثة" في المرتبة الأولى، حيث التزم بذلك ١٣٤ تطبيق بنسبة (٨٧,٦٪)، في حين لم يفصح (١٩) تطبيق بنسبة (١٢,٤٪) عن مشاركة المعلومات مع أطراف ثالثة وليس معنى ذلك أن تلك التطبيقات لا تشارك بيانات المستخدمين مع جهات خارجية فهي لم تنفي ذلك.

- جاء في المرتبة الثانية بند" تنص سياسة الخصوصية بوضوح وبشكل حصري على برمجيات تحليل الويب التي يستخدمها التطبيق للتتبع والتحليل" فقد أفصح عن ذلك (١٠٦) تطبيق بنسبة (٦٩,٣٪) حيث جاء في سياسات الخصوصية لتلك التطبيقات أنها تستخدم برامج لتتبع وجمع وتحليل البيانات الخاصة بحركة المرور للتطبيق وأدائه مثل أداة التحليل google analytics، كما ذكرت بعض التطبيقات أنها تستخدم أيضا أداة Firebase، وترى الباحثة أن تلك البرمجيات تؤثر على خصوصية المستخدمين وكان الأحرى لمطوري تلك التطبيقات استخدام برمجيات توفر خيارات لحماية الخصوصية مثل برمجية Motomo Analytics مفتوحة المصدر والتي توفر مستوى عال جدا من الخصوصية، بينما لم يفصح (٤٧) تطبيق بنسبة (٣٠,٧٪) عن برمجيات تحليل الويب التي يستخدمها واكتفت فقط بذكر عبارة[نحن نستخدم مزودي الخدمة التابعين لجهات خارجية لمراقبة وتحليل استخدام خدمتنا] دون ذكر البرمجيات والأدوات المستخدمة في ذلك.

- ويأتي بند" تنص سياسة الخصوصية بوضوح على أسباب مشاركة البيانات مع أطراف ثالثة" في المرتبة الثالثة، حيث استعرض (٦٨) تطبيق بنسبة (٤٤,٤٪) أسباب مشاركة البيانات مع أطراف وجهات خارجية بطريقة محددةً وواضحة حيث ذكرت الجهة الخارجية وأسباب مشاركة البيانات معها ونوع البيانات التي تشاركها كل على حدة، بينما ذكر (٥٣) تطبيق بنسبة (٣٤,٦٪) أسباب المشاركة ولكن بطريقة عامة ومبهمة مثل [لتيسير خدماتنا، من أجل تزويدك بخدمة ومنتج أفضل، لتقديم الخدمة نيابة عنا، لمساعدتنا في تحليل كيفية استخدام خدمتنا، للامتثال للالتزامات القانونية، لأغراض تسويقية، لغرض البحث العلمي والأكاديمي، نقل الملكية] وأكثر ما أثار قلق الباحثة في هذا هو عبارة "نقل الملكية" حيث صرحت بعض التطبيقات أنه في حالة بيع الأصول أو الدمج مع شركة أخرى فقد يكشف مقدمو الخدمة عن بيانات المستخدمين الشخصية والحساسة لأنها حينئذ تُعد من الأصول المنقولة، دون أن تنوه إلى أنها ستُخطر المستخدم بذلك وتطلب موافقته، ومعنى ذلك أن يخضع المستخدم لسياسة خصوصية جديدة ليس على علم بها، بينما لم يفصح (٣٢) تطبيق بنسبة (٢٠,٩٪) عن أسباب مشاركة البيانات، فهناك(١٩) تطبيق لم يفصح أساسا عن مشاركته البيانات مع أطراف ثالثة، و(١٣) تطبيق ذكرت أنها تشارك البيانات مع جهات خارجية دون ذكر الغرض من الكشف عن البيانات.

- تلا ذلك في المرتبة الرابعة بند" تحدد سياسة الخصوصية بوضوح الأطراف الثالثة بشكل حصري" حيث استعرض (٦٤) تطبيق بنسبة (٤١,٨٪) الجهات الخارجية التي تشارك البيانات معها بشكل حصري مثل(Apple HealthKit, Google Fit, Google Ads, Amazon Web services, Analytical tools) وذكرت أنها لن تشارك البيانات مع أطراف أخرى بخلاف المذكورة في سياسة الخصوصية، بينما التزام (٢٨) تطبيق بنسبة (١٨,٣٪) بهذا البند جزئيا حيث لم تفصح صراحة عن تلك الجهات واكتفت بعبارات مثل(شركاء العمل، المعلنون،

مقدمى خدمات التخزين السحابي، المنصات الاجتماعية، أو بعبارات مثل على سبيل المثال وليس الحصر)، بينما لم يكشف (٦١) تطبيق بنسبة (٣٩,٩٪) عن هذه الأطراف مطلقا.

- وبالنسبة لبند" تتسم بنود سياسة الخصوصية بالوضوح والشفافية في صياغة أحكام مشاركة البيانات مع أطراف ثالثة" فقد جاء في المرتبة الخامسة، حيث جاءت أحكام مشاركة البيانات مع أطراف ثالثة واضحة في (٣٤) تطبيق فقط بنسبة (٢٢,٢٪) فقد جاء في بيان الخصوصية لتلك التطبيقات ما إذا كانت تشارك المعلومات الشخصية للمستخدمين مع الأطراف الثالثة أم أنها تشارك فقط معلومات غير محددة الهوية، وذكرت أن تلك الأطراف ملزمة بعدم الكشف عن المعلومات أو استخدامها لأي غرض آخر، بينما جاءت واضحة جزئيا في (٤٩) تطبيق بنسبة (٣٢٪) حيث لم تقيد بنصا صريحا صلاحيات الأطراف الثالثة في عدم استخدام البيانات لأى غرض آخر غير منصوص عليه في سياسة الخصوصية، في حين لم يستعرض (٧٠) تطبيق بنسبة (٤٥,٨٪) نهائيا أحكام مشاركة البيانات مع الأطراف الثالثة، والأمر المثير للدهشة أن الغالبية العظمى من التطبيقات قامت بإخلاء مسئوليتها عن تلك الجهات والأطراف الخارجية حيث ذكرت في بيان الخصوصية [ننصحك بشدة بمراجعة سياسات الخصوصية لتلك الجهات، لا نتحمل أي مسؤولية عن محتوى أو ممارسات أي مواقع أو خدمات تابعة لجهات خارجية]، إذا فمستخدم التطبيق مُطالب بقراءة وفهم سياسات الخصوصية لعدد كبير من المواقع ومقدمي الخدمات حتى يطمئن على خصوصيته أثناء استخدام تطبيق واحد، وهو فيما اعتقد أمر محال، ومن ثم ترى الباحثة أنه بدلا من أن يُخلى مطورو التطبيقات مسئوليتهم عن الأطراف الثالثة يجدر بهم صياغة عقود صارمة بينهم وبين تلك الجهات تُحافظ على خصوصية المستخدم وتمنعهم من إساءة استخدام البيانات، وأن تُعلن بنودها للمستخدم في سياسة الخصوصية للتطبيق.
- وفي المرتبة السادسة يأتي بند" تنص سياسة الخصوصية على التزام مقدمو الخدمة بعدم الإفصاح عن أي من البيانات والمعلومات الخاصة بالمستخدم لأي من جهات تنفيذ القانون إلا في حالة وجود أمر قضائي مسبق" حيث صرح بذلك (٤٩) تطبيق بنسبة (٣٢٪) فقد صرحت تلك التطبيقات بأنها قد تفصح عن بيانات المستخدم الشخصية للامتثال للقوانين أو أوامر المحكمة، في حين أغفل (١٠٤) تطبيق بنسبة (٦٨٪) توضيح ذلك أو الإشارة إليه.
- ويأتي بعد ذلك في المرتبة السابعة بند" تنص سياسة الخصوصية على أن مشاركة البيانات مع أطراف ثالثة تستند إلى موافقة مسبقة من المستخدم" حيث صرح (٢٤) تطبيق فقط بنسبة (١٥,٧٪) بهذا البند جزئيا حيث جعلت تلك التطبيقات موافقة المستخدم الصريحة على مشاركة البيانات مع جهات خارجية مطلوبة فقط لنوعيات معينة من البيانات مثل (البيانات الحساسة، والبيانات الجينية، مشاركة البيانات مع شركات الإعلانات، أو في حال استخدام البيانات في أغراض غير منصوص عليها في سياسة الخصوصية) أما البيانات الشخصية وبيانات الاستخدام فيتم الكشف عنها بدون إذن المستخدم، في حين لم يطلب (١٢٩) تطبيق بنسبة (٨٤,٣٪) موافقة المستخدم الصريحة على مشاركة بياناته مع جهات خارجية، فقد اكتفوا بعبارة [أن استخدامك للتطبيق يعني أنك قرأت ووافقت على سياسة الخصوصية] وهذا يعني موافقته على الكشف عن بياناته.
- وأخيرا يأتي في المرتبة الثامنة بند" تنص سياسة الخصوصية على التزام مقدمو الخدمة بعدم نقل البيانات الشخصية للمستخدم التي تم جمعها ومعالجتها إلى دولة أخرى إلا بعد الموافقة الصريحة من المستخدم" حيث توافر هذا البند جزئيا في (١٢) تطبيق بنسبة (٧,٨٪) فقط، حيث حرصت تلك التطبيقات على إبلاغ المستخدم بأنه من الممكن نقل بياناته ومعالجتها وتخزينها في دولة

أخرى بخلاف دولته حيث مكان وجود خوادم الشركة مثل (الولايات المتحدة، المملكة المتحدة، الهند، إسرائيل)، بينما لم تطلب الموافقة الصريحة من المستخدم واكتفت بعبارة [إن موافقتك على سياسة الخصوصية وتقديمك لبياناتك الشخصية يُعد موافقة على النقل]، كما لم تُفصح عن الآليات والتدابير الوقائية التي تتبناها لضمان خصوصية البيانات الشخصية عند النقل لدولة أخرى، في حين لم يكشف (١٤١) تطبيق بنسبة (٩٢,٢٪) عن هذا البند على الإطلاق، ولم تحدد أماكن خوادم الشركة المسئولة عن التطبيق والتي يتم بها معالجة وتخزين البيانات والتي قد تكون دولة لا يتوافر بها قانون لحماية البيانات الشخصية أو لا يتوافر بها نفس مستوى الحماية المتاحة في دولة المستخدم، وبذلك فإن جميع تطبيقات الصحة المتنقلة عينة الدراسة لم تلتزم بقوانين الخصوصية في هذا الأمر، حيث تنص المادة (١٤) من القانون ١٥١ لسنة ٢٠٢٠ بحظر إجراء عمليات نقل للبيانات الشخصية إلى دولة أجنبية إلا بتوافر مستوى من الحماية لا يقل عن المستوى المنصوص عليه في هذا القانون، وتنص المادة (١٥) من نفس القانون أنه يجوز في حالة الموافقة الصريحة للشخص المعني بالبيانات نقل البيانات إلى دولة لا يتوافر فيها نفس مستوى الحماية، وبذلك لم تلتزم جميع تطبيقات الصحة المتنقلة عينة الدراسة بطلب موافقة المستخدم الصريحة على النقل إلى دولة أخرى.

خامسا: تأمين البيانات:

تُلزم لوائح وقوانين الخصوصية معالجو البيانات الشخصية بضرورة اتخاذ التدابير التقنية والتنظيمية للتأكد من حماية خصوصية البيانات الشخصية، فلابد أن يسعى مقدمو الخدمة في تطبيقات الصحة المتنقلة إلى تأمين وحماية بيانات المستخدمين التي يقومون بجمعها وتخزينها ومعالجتها، مع الكشف من خلال سياسات الخصوصية عن جهودهم في ذلك وإجراءاتهم في منع أي عملية اختراق أو انتهاك لتلك البيانات، ويوضح الجدول رقم (٩) ممارسات تطبيقات الصحة المتنقلة في تأمين بيانات المستخدمين.

جدول رقم (٩): مستوى امتثال تطبيقات الصحة المتنقلة عينة الدراسة لأفضل ممارسات تأمين البيانات

البنود	نعم		جزئيا		لا		المتوسط الحسابي	الترتيب
	ت	النسبة٪	ت	النسبة٪	ت	النسبة٪		
تنص سياسة الخصوصية على خضوع التطبيق لجميع التدابير المتاحة لضمان جمع وتخزين ومعالجة البيانات والمعلومات بشكل آمن ووفقا لسياسة الخصوصية التي وافق عليها المستخدم	44	28.8%	58	37.9%	51	33.3%	0.48	1
تنص سياسة الخصوصية على حق المستخدم في استخدام بروتوكولات التشفير سواء في نقل أو تخزين البيانات كلما أمكن ذلك	17	11.1%			136	88.9%	0.11	2
تقدم سياسة الخصوصية توصيات للمستخدم بالاعتماد على برمجيات حماية للخصوصية مثل الشبكات الخاصة الافتراضية VPN	4	2.6%			149	97.4%	0.03	3
المتوسط الحسابي العام	0.20							

كما هو موضح بالجدول رقم (٩) فإن كشف تطبيقات الصحة المتنقلة عينة الدراسة عن ممارساتهم فيما يتعلق بمحور تأمين البيانات جاء ضعيفا بمتوسط حسابي بلغ (٠,٢٠)، فلم تكشف غالبية التطبيقات عينة الدراسة عن آليات أمن المعلومات التي تتخذها لحماية خصوصية البيانات الشخصية للمستخدمين، ومن تحليل بيانات الجدول يتضح أن:

- جاء بند" تنص سياسة الخصوصية على خضوع التطبيق لجميع التدابير المتاحة لضمان جمع وتخزين ومعالجة البيانات والمعلومات بشكل آمن ووفقا لسياسة الخصوصية التي وافق عليها المستخدم" في المرتبة الأولى، حيث حرص (٤٤) تطبيق فقط بنسبة (٢٨,٨٪) على الإفصاح عن التدابير التي تتخذها لحماية بيانات المستخدم، حيث ذكرت بعض التطبيقات أنها تستخدم بروتكول التشفير Secure Socket Layer(SSI) وبروتكول Transport layer Security(TLS) في تشفير وتعمية البيانات الشخصية والحساسة عند النقل والإرسال، كما اعتمد بعض منها في تشفير كل عملية نقل للبيانات الشخصية باستخدام بروتكول نقل النص التشعبي الآمن Hyper Text Transfer Protocol Secure(HTTPS)، كما ذكر تطبيق واحد فقط بأنه استوفى متطلبات معيار Iso27001 الخاص بإدارة أمن المعلومات، هذا فضلا عن تدابير أخرى كالجدران النارية، في حين صرح (٥٨) تطبيق بنسبة (٣٧,٩٪) عن تدابير الحماية جزئيا حيث جاء في بيان الخصوصية لتلك التطبيقات(نسعى جاهدين لاستخدام وسائل مقبولة تجاريا لحماية بياناتك الشخصية، لا يمكننا ضمان أمانها المطلق، وتذكر دائما أنه لا توجد طريقة نقل عبر الإنترنت، أو طريقة للتخزين الالكتروني آمنة بنسبة ١٠٠٪) فهي أعلمت المستخدم أنها تسعى لحماية بياناته الشخصية دون أن تُحدد التدابير التقنية والتنظيمية المستخدمة لحماية البيانات الشخصية على وجه التحديد وفي نفس الوقت أخلت مسؤوليتها عن أي عملية اختراق أو انتهاك للبيانات حينما ذكرت أنه لا يمكنها القضاء تماما على المخاطر الأمنية المرتبطة بتخزين ونقل البيانات، هذا وقد أغفل (٥١) تطبيق بنسبة (٣٣,٣٪) هذا البند نهائيا حيث لم تكشف في بيان الخصوصية عن أية معلومات تتعلق بحماية بيانات المستخدم الشخصية والحساسة.
- وفي المرتبة الثانية جاء بند" تنص سياسة الخصوصية على حق المستخدم في استخدام بروتكولات التشفير سواء في نقل أو تخزين البيانات كلما أمكن ذلك" حيث أوصى (١٧) تطبيق فقط بنسبة (١١,١٪) المستخدم بأهمية أن يقوم بتشفير بياناته الشخصية أثناء الإرسال وبضرورة اختيار كلمات مرور قوية للتطبيق، بينما تجاهل (١٣٦) تطبيق بنسبة (٨٨,٩٪) هذا البند نهائيا.
- وجاء بند" تقدم سياسة الخصوصية توصيات للمستخدم بالاعتماد على برمجيات حماية للخصوصية مثل الشبكات الخاصة الافتراضية VPN" حيث وردت توصيات بذلك في (٤) تطبيقات فقط بنسبة (٢,٦٪) وهذا من شأنه تشفير حركة مرور البيانات مما يمنح المستخدم قدراً أكبر من الخصوصية والحماية لسرية بياناته وهويته، في حين لم يقدم (١٤٩) تطبيق بنسبة (٩٧,٤٪) أية توصيات بخصوص ذلك.

سادسا: حق المستخدم وسيطرته على بياناته:

تسعى قوانين ولوائح خصوصية البيانات إلى تمكين أصحاب البيانات ومنحهم القدرة على التحكم في بياناتهم الشخصية أو ما يسمى بحقوق الشخص المعني بالبيانات، فوفقا للمادة (٢) من القانون ١٥١ لسنة ٢٠٢٠، والمادة (١٧) و(٢٠) من اللائحة العامة لحماية البيانات، يكون للشخص المعني بالبيانات الحق في السيطرة على بياناته، كالحق في محوها والعدول عن الموافقة على معالجتها، والحق في طلب نسخة منها والحصول عليها، ويوضح الجدول رقم (١٠) مدى التزام تطبيقات الصحة المتنقلة عينة الدراسة بالكشف عن حقوق المستخدم وسلطته في السيطرة على بياناته.

جدول رقم (١٠): مستوى امتثال تطبيقات الصحة المتنقلة عينة الدراسة لأفضل ممارسات حق المستخدم في السيطرة على بياناته

البنود	نعم		جزئيا		لا		المتوسط الحسابي	الترتيب
	ت	النسبة٪	ت	النسبة٪	ت	النسبة٪		
تنص سياسة الخصوصية على حق المستخدم في طلب إلغاء اشتراكه في أي وقت، ويلتزم التطبيق بإلغاء الاشتراك	61	39.9%	15	9.8%	77	50.3%	0.45	1
تنص سياسة الخصوصية على حق المستخدم في طلب محو بياناته ومعلوماته الشخصية في أي وقت، ويلتزم التطبيق بذلك.	62	40.5%	11	7.2%	80	52.3%	0.44	2
تنص سياسة الخصوصية على حق المستخدم في طلب نسخة من جميع البيانات والمعلومات الخاصة به في أي وقت دون شرط إبداء أسباب.	59	38.6%	2	1.3%	92	60.1%	0.39	3
المتوسط الحسابي العام	0.43							

حيث يتبين من الجدول رقم (١٠) أن التزام واعتراف تطبيقات الصحة المتنقلة عينة الدراسة بحق المستخدم في بياناته وسيطرته عليها والكشف عن بنود ذلك جاء متوسطا بمتوسط حسابي بلغ (٠,٤٣)، ويمكن توضيح ذلك فيما يلي:

- جاء بند" تنص سياسة الخصوصية على حق المستخدم في طلب إلغاء اشتراكه في أي وقت، ويلتزم التطبيق بإلغاء الاشتراك" في المرتبة الأولى، حيث اعترف (٦١) تطبيق بنسبة (٣٩,٩٪) بحق المستخدم في الغاء اشتراكه في التطبيق ويلتزم التطبيق بحذف بيانات المستخدم، وإذا تم الاحتفاظ بالبيانات فسيتم الاحتفاظ بها في صورة لا تسمح بتحديد هوية المستخدم، بينما صرح (١٥) تطبيق بنسبة (٩,٨٪) بحق المستخدم في الغاء اشتراكه ولكن مع الاحتفاظ ببياناته الشخصية لفترة زمنية معينة، حيث جاء في بيان الخصوصية لبعض التطبيقات[إذا اخترت حذف التطبيق من جهازك أو أصبح حسابك غير نشط، فسنحتفظ ببياناتك الشخصية لمدة ٣ سنوات] بينما صرح البعض بأنه قد يحتفظ بالبيانات الشخصية لمدة ٦ أشهر وفي البعض مدة لا تزيد عن ٣٠ يوما، دون أن تكشف عن أسباب الاحتفاظ بالبيانات لهذه الفترات كالالتزامات القانونية مثلا، والغريب في الأمر ما صرحت به سياسة الخصوصية لتطبيق ما بأنه [يمكنك حذف حسابك، وسيظل النشاط الذي تم إنشاؤه قبل الحذف مخزنا من قبلنا وقد يكون متاحا للجمهور] فقد اعترف بحق المستخدم في إنهاء اشتراكه ولكن ستظل بياناته مسجلة لديهم لفترة غير محددة، والاحتفاظ بالبيانات لهذه الفترات الطويلة مخالف لقوانين حماية البيانات الشخصية مادام ليس له مبرر قانوني، حيث تنص المادة (٣) من القانون ١٥١ لسنة ٢٠٢٠ أنه "يُشترط لمعالجة البيانات الشخصية توافر مجموعة من الشروط ومنها ألا يتم الاحتفاظ بها لفترات أطول من المدة اللازمة للوفاء بالغرض المحدد لها"، فإذا كان المستخدم نفسه لم يُعد بحاجة للخدمات التي يقدمها التطبيق فما الداعي من وراء الاحتفاظ ببياناته الشخصية بعد انتهاء الاحتياج إليها، هذا وقد أغفل (٧٧) تطبيق بنسبة (٥٠,٣٪) حق المستخدم في ذلك ولم يرد ذكره مطلقا.
- وفي المرتبة الثانية جاء بند" تنص سياسة الخصوصية على حق المستخدم في طلب محو بياناته ومعلوماته الشخصية في أي وقت، ويلتزم التطبيق بذلك" حيث صرح (٦٢) تطبيق بنسبة (٤٠,٥٪) بأنه من حق المستخدم أن يطلب حذف بياناته في أي وقت، بينما صرح (١١) تطبيق بنسبة (٧,٢٪) بهذا الحق جزئيا حيث صرحت تلك التطبيقات أنها ستبذل جهودا لتلبية طلب

المستخدم في حذف بياناته، ولكنها قد تحتفظ بنسخة مؤرشفة إذا طُلب ذلك بموجب القانون أو لأغراض تجارية مشروعة، كما جاءت في بعض التطبيقات بأن الحق في حذف البيانات ليس مطلقا وقد يحق لهم رفض الطلب جزئيا أو كليا، بينما لم يتعرض (٨٠) تطبيق بنسبة (٥٢,٣٪) لحق المستخدم في طلب محو بياناته نهائيا. وهنا تذكرت الباحثة عبارة (الانترنت يسجل كل شيء ولا ينسى أبدا) التي ذكرها جيفري روسن Jeffery Rosen عام ٢٠١٠ والتي حملت مخاوف لدى الأفراد من استمرار الاحتفاظ ببياناتهم وعدم قدرتهم على حذفها.

- وجاء في المرتبة الثالثة" تنص سياسة الخصوصية على حق المستخدم في طلب نسخة من جميع البيانات والمعلومات الخاصة به في أي وقت ودون شرط إبداء أسباب" حيث التزم (٥٩) تطبيق بنسبة (٣٨,٦٪) بحق المستخدم في طلب نسخة قابلة للقراءة ومنظمة من بياناته، ويكون ذلك بمقابل تكلفة الخدمة، بينما صرح (٢) تطبيق بنسبة (١,٣٪) بذلك جزئيا حيث ذكرت بأن من حق المستخدم طلب نسخة من بياناته ولكن قد يحق لهم رفض الطلب حيثما تنطبق الاستثناءات بموجب القانون المعمول به، بينما لم يعرض (٩٢) تطبيق بنسبة (٦٠,١٪) حق المستخدم في ذلك.

سابعا: الإبلاغ عن تعديل أو تحديث سياسة الخصوصية:

إن الغرض من سياسات الخصوصية للتطبيقات والمواقع هو ضمان إلمام المستخدم بالكيفية التي يقوم بها التطبيق بجمع بياناته الشخصية ومعالجتها، والتعريف بممارسات خصوصية البيانات المُطبقة، إلا أن هذه السياسات لابد ان تخضع للتحديث والمراجعة دوريا حتى تتماشى مع التطور في مجال البرمجيات وكذلك التطور في الخدمات التي يقدمها التطبيق، والسؤال هنا هل يلتزم مطورو تطبيقات الصحة المتنقلة بإبلاغ المستخدم بأية تعديلات قد أجريت على سياسة الخصوصية قبل أن تُدخلها حيز التنفيذ، حتي يتمكن المستخدم من اتخاذ القرار المستنير بشأن الاستمرار في استخدام التطبيق من عدمه. وهو ما يوضحه الجدول رقم (١١).

جدول رقم (١١): مستوى امتثال تطبيقات الصحة المتنقلة عينة الدراسة لأفضل ممارسات الإبلاغ عن تحديث سياسة الخصوصية

البنود	نعم		جزئيا		لا		المتوسط الحسابي	الترتيب
	ت	النسبة٪	ت	النسبة٪	ت	النسبة٪		
تنص سياسة الخصوصية على التزام مطورو التطبيق بإبلاغ المستخدم عن أية تعديلات في سياسة الخصوصية عن طريق البريد الالكتروني أو الصفحة الرئيسية للتطبيق قبل إدخال التعديلات حيز التطبيق	96	62.7%			57	37.3%	0.63	1
تنص سياسة الخصوصية على التزم مطورو التطبيق بالحصول على موافقة المستخدم قبل تطبيق أية تعديلات في سياسة الخصوصية	1	0.7%	3	2.0%	149	97.4%	0.02	2
المتوسط الحسابي العام	0.32							

حيث يتبين من الجدول رقم (١١) أن التزام تطبيقات الصحة المتنقلة عينة الدراسة بالكشف عن ممارساتهم فيما يتعلق بإبلاغ المستخدم عن التغييرات التي تطرأ على سياسات الخصوصية للتطبيقات جاء ضعيفا بمتوسط حسابي بلغ (٠,٣٢)

- وقد جاء بند" تنص سياسة الخصوصية على التزام مطورو التطبيق بإبلاغ المستخدم عن أية تعديلات في سياسة الخصوصية عن طريق البريد الالكتروني أو الصفحة الرئيسية للتطبيق قبل إدخال التعديلات حيز التنفيذ" في المرتبة الأولى، حيث صرح بذلك (٩٦) تطبيق بنسبة (٦٢,٧٪)، فقد صرحت تلك التطبيقات بأن من حقها تعديل وتحديث سياسة الخصوصية من وقت لآخر، وإذا حدث ذلك فستقوم بنشر السياسة الجديدة على الصفحة الرئيسية بتاريخ التحديث قبل أن تُصبح التعديلات سارية المفعول بثلاثين يوماً، بينما صرح عدد قليل من التطبيقات بأنها ستقوم بإخطار المستخدم بسياسة الخصوصية الجديدة بإرسال بريد إلكتروني إليه، في حين لم يكشف (٥٧) تطبيق بنسبة (٣٧,٣٪) عن ممارساته فيما يتعلق بأمر تعديل سياسة الخصوصية.
- وجاء في المرتبة الثانية بند" تنص سياسة الخصوصية على التزام مطورو التطبيق بالحصول على موافقة المستخدم قبل تطبيق أية تعديلات في سياسة الخصوصية"، حيث صرح تطبيق واحد فقط بنسبة (٠,٧٪) بأنه سيعطى المستخدم خيار الموافقة الصريحة على التغييرات التي تطرأ على سياسة الخصوصية، بينما صرح (٣) تطبيقات بنسبة (٢٪) بذلك جزئيا حيث ذكرت تلك التطبيقات أن استمرار المستخدم في استخدام الخدمة بعد التاريخ الفعلي للإصدار المُحدث يعنى موافقته على سياسة الخصوصية بصيغتها المنقحة، في حين لم يتعرض (١٤٩) تطبيق بنسبة (٩٧,٤٪) لهذا البند على الإطلاق.

ثامنا :الإبلاغ عن تسريب البيانات:

رغم الاحتياطات التي قد يتخذها مقدمو الخدمة، إلا أنه قد يحدث اختراق للبيانات، وهنا لابد أن يلتزم مقدمو الخدمة امتثالا للوائح وقوانين الخصوصية بإبلاغ المستخدم عن أي انتهاك أو تعدي أو تسريب تتعرض له بياناته الشخصية والتي تؤثر بالتأكيد على خصوصيته، حيث تنص المادة (٢) من القانون ١٥١ لسنة ٢٠٢٠ بأن للشخص المعني بالبيانات الحق في العلم والمعرفة بأي خرق أو انتهاك لبياناته الشخصية، ويكشف الجدول رقم (١٢) عن الممارسات التي يتخذها مقدمو الخدمة في تطبيقات الصحة المتنقلة إذا حدث أي اختراق لبيانات المستخدم.

جدول رقم (١٢): مستوى امتثال تطبيقات الصحة المتنقلة عينة الدراسة لأفضل ممارسات الإبلاغ عن تسريب البيانات

البنود	نعم		جزئيا		لا		المتوسط الحسابي	الترتيب
	ت	النسبة٪	ت	النسبة٪	ت	النسبة٪		
تنص سياسة الخصوصية على التزم مقدمو الخدمة بإبلاغ المستخدم عن أي تسريب للبيانات والمعلومات التي تم جمعها وتخزينها.	7	4.6%	2	1.3%	144	94.1%	0.05	1
تنص سياسة الخصوصية على التزام مقدمو الخدمة بإبلاغ المستخدم بالضرر الذي يمكن أن يطال خصوصيته بسبب تسريب البيانات					153	100.0%	0.00	2
المتوسط الحسابي العام	0.03							

حيث يتضح من الجدول رقم (١٢) أن التزام مقدمو الخدمة لتطبيقات الصحة المتنقلة عينة الدراسة بالكشف عن ممارساتهم فيما يتعلق بإبلاغ المستخدم عما تتعرض له بياناته من اختراق أو تسريب أو انتهاك جاء ضعيفا بمتوسط حسابي بلغ (٠,٠٣).

- وقد جاء بند" تنص سياسة الخصوصية على التزام مقدمو الخدمة بإبلاغ المستخدم عن أي تسريب للبيانات والمعلومات التي تم جمعها وتخزينها" في المرتبة الأولى، حيث صرحت (٧) تطبيقات بنسبة (٤,٦٪) بأنه في حالة حدوث اختراق لبيانات المستخدم فسيتم إخطاره عبر البريد الالكتروني خلال ٧٢ ساعة، وفي بعض التطبيقات خلال ٧ أيام عمل، وصرح (٢) تطبيق بنسبة (١,٣٪) بذلك جزئيا حيث ذكرت أنه في حالة وقوع حادث أمني ستقوم بإبلاغ السلطات المختصة ولم تذكر المستخدم، كما لم يكشف (١٤٤) تطبيق بنسبة (٩٤,١٪) عن ممارساته فيما يتعلق بأمر إبلاغ المستخدم عن تسريب البيانات نهائيا.
- وجاء في المرتبة الثانية بند" تنص سياسة الخصوصية على التزام مقدمو الخدمة بإبلاغ المستخدم بالضرر الذي يمكن أن يطال خصوصيته بسبب تسريب البيانات"، حيث لم يصرح أي تطبيق من تطبيقات الصحة المتنقلة عينة الدراسة بهذا مطلقا.

٣/٣ الدراسة الميدانية:

تستعرض الدراسة هنا واقع استخدام تطبيقات الصحة المتنقلة ومدى وعي مستخدميها بآليات حماية الخصوصية على عينة من المستخدمين من المجتمع المصري والتي تم استجابتها كعينة عشوائية من خلال طرح استبانة إلكترونية على جوجل درايف Google drive حيث استجابت عينة قدرت ب ٢١٠ مفردة.

أولا: وصف العينة: البيانات الديموجرافية:

يوضح الجدول التالي عرضا وصفيا لعينة الدراسة وفقا لعدة متغيرات .

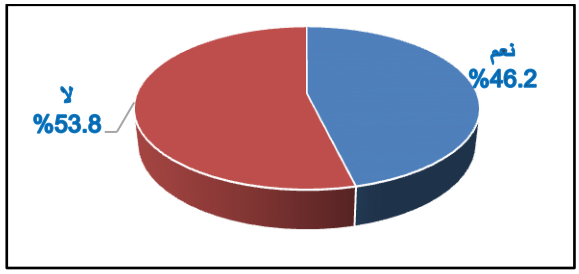
جدول (١٣): توزيع عينة الدراسة وفقا للمتغيرات الديموجرافية

المتغير		ك	%
الفئة العمرية	18-29	41	19.5%
	30-39	69	32.9%
	40-49	83	39.5%
	50-59	14	6.7%
	> 60	3	1.4%
النوع	ذكور	116	55.2%
	أناث	94	44.8%
المؤهل الدراسي	أقل من ثانوي	9	4.3%
	ثانوية عامة أو ما يعادلها	68	32.4%
	جامعي	109	51.9%
	مؤهل فوق جامعي	24	11.4%
نظام التشغيل للهاتف المحمول	نظام Android	192	91.4%
	نظام IOS	18	8.6%

حيث يتضح من الجدول رقم (١٣) تباين خصائص العينة المشاركة في الاستبانة، فوفقا لنوع الجنس، بلغ عدد الذكور ١١٦ بنسبة (٥٥,٢٪)، بينما بلغ عدد الإناث ٩٤ بنسبة بلغت (٤٤,٨٪). كما يتضح توزيع عينة الدراسة المشاركة وفقا للفئة العمرية، والتي قسمتها الباحثة إلي خمس فئات عمرية، جاء في مقدمتها الفئة العمرية من سن(٤٠-٤٩) بعدد ٨٣ مشارك بنسبة (٣٩,٥٪)، يليها الفئة العمرية (٣٠-٣٩ سنة) بعدد ٦٩ مشارك بنسبة (٣٢,٩٪). وجاءت في المرتبة الثالثة الفئة العمرية من (١٨-٢٩ سنة) بعدد ٤١ بنسبة

(١٩,٥٪)، وفي المرتبة الرابعة الفئة العمرية من (٥٠-٥٩ سنة) بنسبة (٦,٧٪). كما شارك ثلاثة فقط من الفئة العمرية (٦٠ سنة فأكثر) في الإجابة علي الاستبانة بنسبة (١,٤٪). أما بالنسبة لتوزيع المشاركين في الدراسة وفقا للمؤهل الدراسي، فقد بلغ عدد الحاصلون علي مؤهل جامعي ١٠٩ بنسبة (٥١,٩٪)، يليهم الحاصلون على مؤهل ثانوي أو ما يعادله حيث بلغ عددهم ٦٨ بنسبة(٣٢,٤٪)، كما بلغ عدد المشاركين الحاصلين على مؤهل فوق جامعي ٢٤ مشارك بنسبة (١١,٤٪)، بينما انخفض عدد المشاركين الحاصلين علي مؤهل أقل من ثانوي حيث بلغ عددهم ٩ أفراد فقط بنسبة (٤,٣٪). كما يتبين أن غالبية المشاركين في الدراسة يستخدمون على هواتفهم نظام التشغيل Android بنسبة (٩١,٤٪)، في مقابل (٨,٦٪) فقط يستخدمون نظام التشغيل IOS.

ثانيا: واقع استخدام عينة الدراسة لتطبيقات الصحة المتنقلة:



شكل رقم (٢): استخدام عينة الدراسة لتطبيقات الصحة المتنقلة

يتضح من الشكل رقم (٢) أن (٩٣) مشارك بنسبة (٤٦,٢٪) أشاروا بأنهم يستخدمون بالفعل تطبيقات الصحة المتنقلة على هواتفهم الذكية، في حين أفاد (١١٣) مشارك بنسبة (٥٣,٨٪) بأنهم لا يستخدمون هذه النوعية من التطبيقات، وهو فارق بسيط بين النسبتين، والجدير بالذكر أن غالبية المستخدمين لتلك التطبيقات كانوا في الفئة العمرية من (٣٠ إلى ٤٩ عاما) ويكشف جدول رقم (١٤) أسباب عدم استخدام بعض أفراد العينة لتطبيقات الصحة المتنقلة.

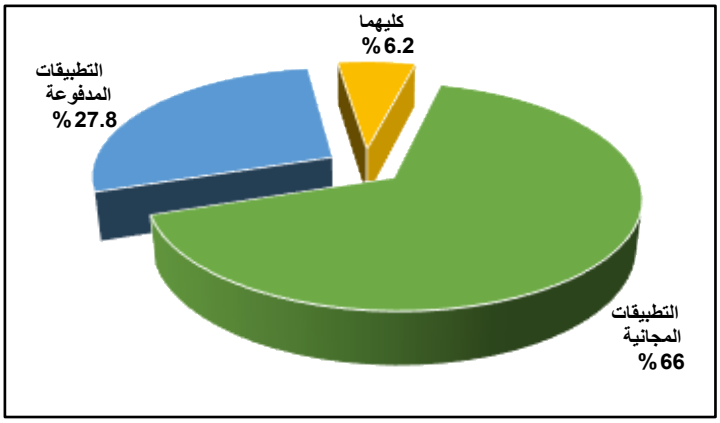
جدول رقم (١٤): أسباب عدم استخدام بعض أفراد العينة لتطبيقات الصحة المتنقلة

أسباب عدم استخدام تطبيقات الصحة المتنقلة	ن=113	
	ك	النسبة٪
لا أعلم بوجود تطبيقات طبية وصحية على متاجر التطبيقات	37	32.7%
أعلم بوجودها، ولكن ليس لدي حاجة إليها	22	19.5%
أفضل أن أسأل مقدمي الرعاية الصحية بشكل مباشر.	57	50.4%
لا أثق فيما تقدمه من معلومات طبية وصحية.	71	62.8%
أقلق بشأن خصوصيتي وأمن البيانات أثناء استخدامها.	42	37.2%
البيانات الصحية بيانات حساسة وأخشى أن تُسئ تلك التطبيقات استخدامها.	42	37.2%
هناك الكثير من الرسائل والإعلانات المزعجة التي اتعرض لها بعد تثبيتها.	24	21.2%

حيث يتبين من استقراء جدول رقم(١٤) أسباب عدم استخدام بعض أفراد العينة لتطبيقات الصحة المتنقلة، والتي تراوحت النسب المئوية لها ما بين (٦٢,٨٪، ١٩,٥٪) حيث أتيحت الفرص لكل فرد من أفراد العينة حرية اختيار أكثر من بديل للإجابة، فمن قراءة الجدول يتضح تفوق المخاوف الصحية لأفراد

العينة على مخاوف الخصوصية، حيث حصلت عبارة" لا أثق فيما تقدمه من معلومات طبية وصحية" على أعلى نسبة موافقة (٦٢,٨٪)، تلاها عبارة" أفضل أن أسأل مقدمي الرعاية الصحية بشكل مباشر" بنسبة موافقة بلغت (٥٠,٤٪)، وحصلت العبارتين" أقلق بشأن خصوصيتي وأمن البيانات أثناء استخدامها" و" البيانات الصحية بيانات حساسة وأخشى أن تُسئ تلك التطبيقات استخدامها" على نسبة موافقة بلغت (٣٧,٢٪) لكل منهما، ومن ثم فهناك نسبة قليلة تُدرك تأثير تلك التطبيقات السلبي على الخصوصية، كما أفادت نسبة (٣٢,٧٪) بأنهم لا يعلمون بوجود تطبيقات طبية وصحية على متاجر التطبيقات، وأشارت نسبة (٢١,٢٪) إلى عبارة" هناك الكثير من الرسائل المزعجة التي اتعرض لها بعد تثبيتها" وقد يشير ذلك إلى أن هؤلاء قاموا بالفعل بتثبيت تطبيقات الصحة المتنقلة على هواتفهم من قبل ولكن قاموا بإلغاء تثبيتها بسبب ما تعرضوا له من رسائل مزعجة وإعلانات، وأخيرا أشارت نسبة (٥.١٩٪) إلى عبارة "أعلم بوجودها، ولكن ليس لدي حاجة إليها".

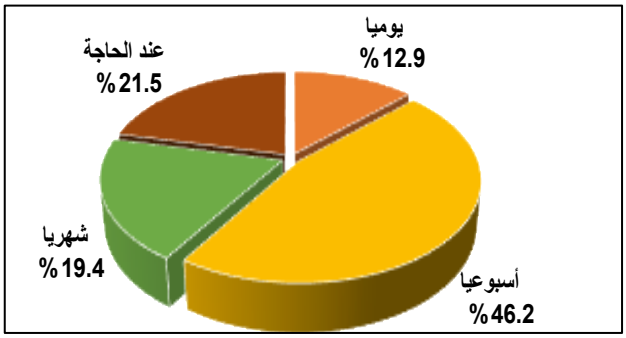
وفيما يلي سوف نركز على المشاركين الذين يستخدمون بالفعل تطبيقات الصحة المتنقلة والبالغ عددهم (٩٣) مشارك بنسبة (٤٦,٢٪) من حجم العينة.



شكل رقم (٣): نوعية تطبيقات الصحة المتنقلة التي يستخدمها أفراد العينة

وكما هو موضح بالشكل رقم (٣) فإن تطبيقات الصحة المتنقلة المجانية جاءت في مقدمة التطبيقات التي يستخدمها أفراد العينة بنسبة (٦٦٪) وهو أمر بديهي ولكنه يشكل خطرا حقيقيا على الخصوصية، فالتطبيقات المجانية تتعامل مع المستخدم ليس باعتباره عميلا بل سلعة فهي تبيع بياناته لجهات أخرى لتحقق بذلك أرباحا هائلة تفوق بكثير ما قد يدفعه المستخدم من مقابل نظير استخدامه للتطبيق، يليها التطبيقات المدفوعة بنسبة (٢٧,٨٪)، بينما أفاد (٦,٢٪) فقط بأنهم يستخدمون كلا النوعين المجانية والمدفوعة.

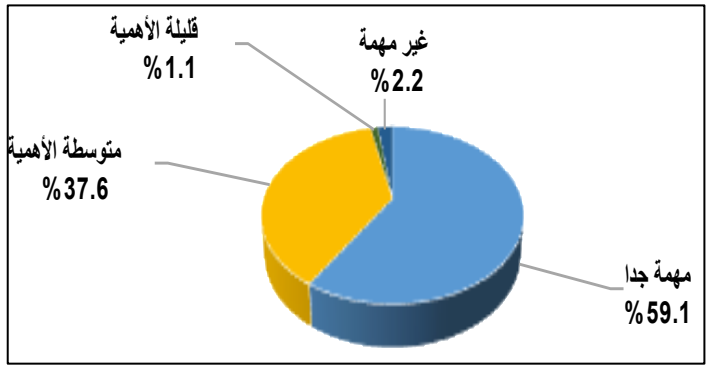
أما عن كثافة استخدام المشاركين في الدراسة لتطبيقات الصحة المتنقلة (ن=٩٣)، فكما هو موضح بالشكل رقم (٤) أن النسبة الأكبر وهي (٤٦,٢٪) من إجمالي عينة الدراسة يستخدمون تطبيقات الصحة المتنقلة أسبوعيا، وهذا يعني أنها أصبحت تمثل لمستخدميها جزءا أساسيا من حياتهم، ومن ثم نستطيع توقع ازدياد الاعتماد عليها على المدى الطويل. مما يؤكد على أهمية نشر ثقافة الاستخدام الآمن لهذه التطبيقات في المجتمع، في حين أن (٢١,٥٪) يستخدمونها عند الحاجة فقط، وأن نسبة (١٩,٤٪) يستخدمون تلك التطبيقات شهريا، وحقق الاستخدام يوميا أقل نسبة من إجمالي العينة وهي (١٢,٩٪).



شكل رقم (): معدل استخدام أفراد العينة لتطبيقات الصحة المتنقلة

ثالثا: اتجاهات عينة الدراسة نحو الخصوصية وممارساتهم لحماية وإدارة خصوصيتهم عبر تطبيقات الصحة المتنقلة:

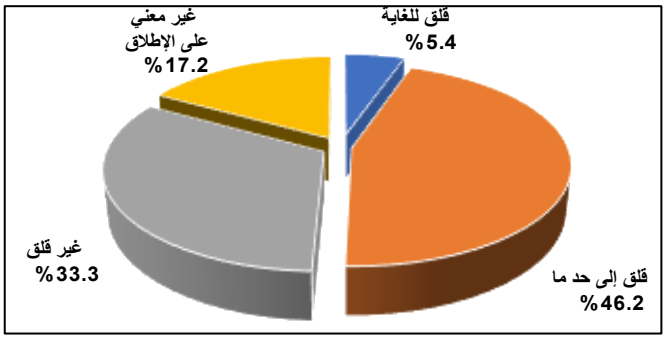
بسؤال مستخدمي تطبيقات الصحة المتنقلة من أفراد العينة عن مدى أهمية الخصوصية الرقمية بالنسبة لهم(ن=٩٣)، فكما هو موضح بالشكل رقم (٥) فقد أفادت النسبة الأكبر وهي(٥٩,١٪) بأنها مهمة جدا، كما أفادت ما نسبته (٣٧,٦٪) بأنها متوسطة الأهمية، وهي نسبة ليست بالقليلة وتُرجع الباحثة ذلك إلى ما أفرزته التقنيات الحديثة، وبصفة خاصة مواقع التواصل الاجتماعي والتي يزداد على صفحاتها مستوى الإفصاح عن الخصوصية، مما جعل الجيل الحالي لا يهتم بمصطلح الخصوصية بل قد يرفضها كقيمة اجتماعية في بعض الأحيان، بينما لم تتعدَ نسبة من أشاروا بأنها غير مهمة نسبة (٢,٢٪)، كما لم تتعدَ نسبة من أفادوا بأنها قليلة الأهمية (١,١٪).



شكل رقم (٥): أهمية الخصوصية الرقمية بالنسبة لمستخدمي تطبيقات الصحة المتنقلة

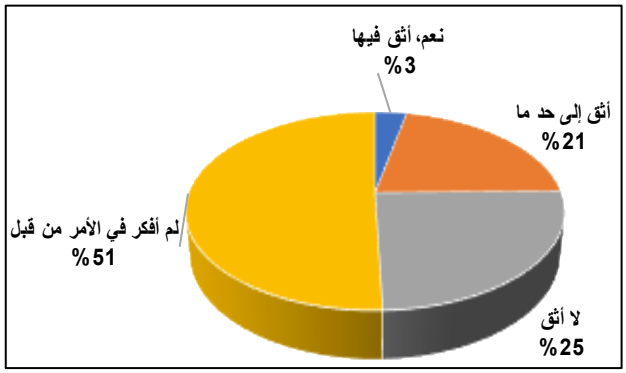
وفيما يتعلق بمدى قلق أفراد العينة المستخدمين لتطبيقات الصحة المتنقلة(ن=٩٣) من توافر معلوماتهم الشخصية والحساسة على تلك التطبيقات، فقد جاءت استجاباتهم كما هو موضح بالشكل رقم (٦) حيث أفاد (٤٦,٢٪) من المستخدمين بأنهم قلقون إلى حد ما، بينما أفاد(٣٣,٣٪) بأنهم غير قلقون، بينما صرحت نسبة (١٧,٢٪) من المستخدمين بأنهم غير معنيين بذلك على الإطلاق، ولم تتعدَ نسبة من أفادوا بأنهم قلقون للغاية (٥,٤٪)، مما يشير إلى جهل المستخدمين بمخاطر الإفصاح عن الخصوصية وعدم

إدراكهم لطبيعة الانتهاك الذي تقوم به هذه التطبيقات، والتي قد تقوم بالاستفادة من معلوماتهم الشخصية وبيعها لجهات أخرى دون موافقتهم المسبقة.



شكل رقم (٦): مستوى قلق مستخدمي تطبيقات الصحة المتنقلة من توافر معلوماتهم الشخصية على تلك التطبيقات

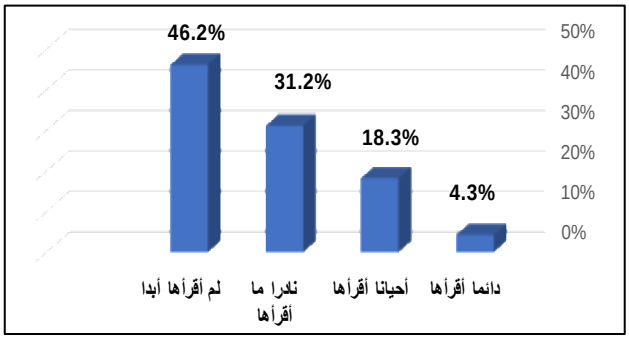
أما عن مستوى ثقة مستخدمي تطبيقات الصحة المتنقلة من أفراد العينة في مستوى تأمين تلك التطبيقات لبياناتهم الشخصية والحساسة، فكما هو مبين بالشكل رقم (٧)، فقد صرح (٥١٪) بأنهم لم يفكروا في الأمر من قبل، وهو الأمر الغريب فقد سبق الذكر أن غالبية المستخدمين كانوا من الفئة العمرية (٣٠ إلى ٤٩) أي أنهم من الجيل الأكثر وعيا من الناحية التكنولوجية ولكن من الواضح أنه وعيا سطحيا، بينما أفادت نسبة (٢٥٪) بأنهم لا يثقون فيها، كما بلغت نسبة من يثقون فيها إلى حد ما (٢١٪)، بينما بلغت نسبة من يثقون فيها (٣٪) فقط.



شكل رقم (٧): مستوى ثقة مستخدمي تطبيقات الصحة المتنقلة في مستوى تأمين تلك التطبيقات لبياناتهم

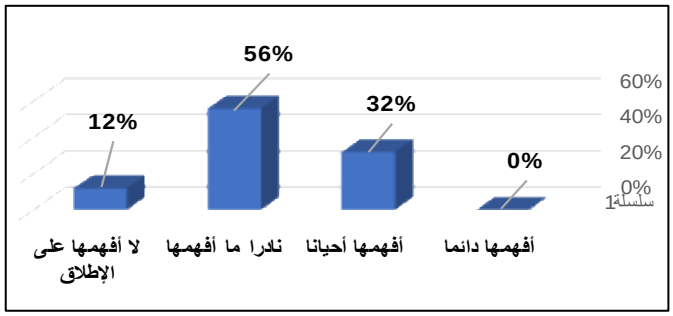
وبسؤال أفراد العينة من مستخدمي تطبيقات الصحة المتنقلة(ن=٩٣) عما إذا كانوا يقرأون سياسات الخصوصية لتلك التطبيقات قبل تثبيتها على هواتفهم المحمولة، فجاءت الاستجابات كما هو موضح بالشكل رقم (٨) أن نسبة (٤٦,٢٪) لم يقرأوها أبدا، مما يؤكد أن الاهتمام بالخصوصية لدى مستخدمي تطبيقات الصحة المتنقلة عينة الدراسة كان نظريا فقط، كما صرحت نسبة (٣١,٢٪) بأنهم نادرا ما يقرأوها، كما أشار ما نسبته (١٨,٣٪) بأنهم أحيانا يقرأوها، بينما انخفضت نسبة من يقرأون سياسة الخصوصية دائما فلم تتعدَ (٤,٣٪)، وربما يرجع عدم اهتمام أفراد العينة بقراءة سياسات الخصوصية لتلك التطبيقات من

وجهة نظر الباحثة إلى أمرين لا ثالث لهما، إما لعدم وعي المستخدمين بأهميتها البالغة في معرفة حقوقهم كمستخدمين وكيف يتعامل التطبيق مع خصوصيتهم، وإما لأنها تُمثل لهم صفحات مملة، وتنصح الباحثة مستخدمي التطبيقات والمواقع بضرورة أن يأخذوا الوقت الكافي لقراءة ومراجعة سياسات الخصوصية لأنها وفقا لما تبين من الدراسة التحليلية تشتمل على بنود تُشكل تعديا صريحا على خصوصية المستخدمين، والتي لو عرفها المستخدم فمن المحتمل أن يغير رأيه حول تثبيت التطبيق.



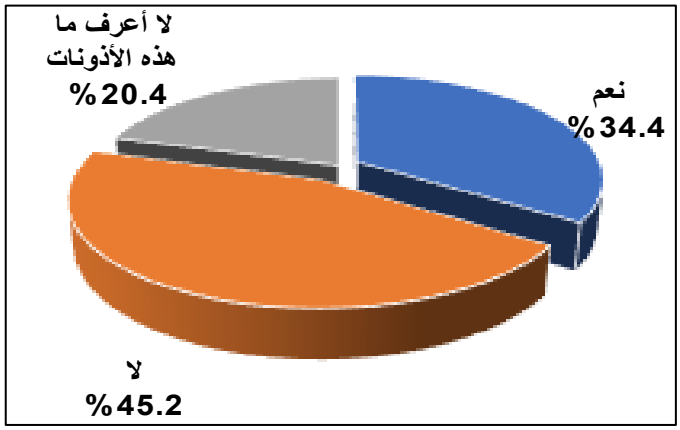
شكل رقم (٨): معدل إطلاع مستخدمي تطبيقات الصحة المتنقلة على سياسات الخصوصية لتلك التطبيقات

ولقد توجهت الباحثة في الاستبانة بسؤال للأفراد المشاركين الذين يقرأون سياسات الخصوصية والبالغ عددهم (٥٠) من إجمالي (٩٣) الذين يمثلون مستخدمي تطبيقات الصحة المتنقلة عما إذا كان يفهمون سياسات الخصوصية بشكل كامل عندما يقرأونها، وقد جاءت استجاباتهم كما هو موضح بالشكل رقم (٩)، فقد صرحت نسبة (٥٦٪) بأنهم نادرا ما يفهمونها، بينما أفادت نسبة (٣٢٪) بأنهم يفهمونها أحيانا، وأشار (١٢٪) بأنهم لا يفهمونها على الإطلاق، بينما انعدمت نسبة من أشاروا إلى أنهم يفهمونها دائما، وهذا يؤكد ما توصلت إليه الدراسة التحليلية بأن غالبية سياسات الخصوصية لتطبيقات الصحة المتنقلة عينة الدراسة جاءت غير واضحة وغير قابلة للفهم من قبل المستخدم العادي.



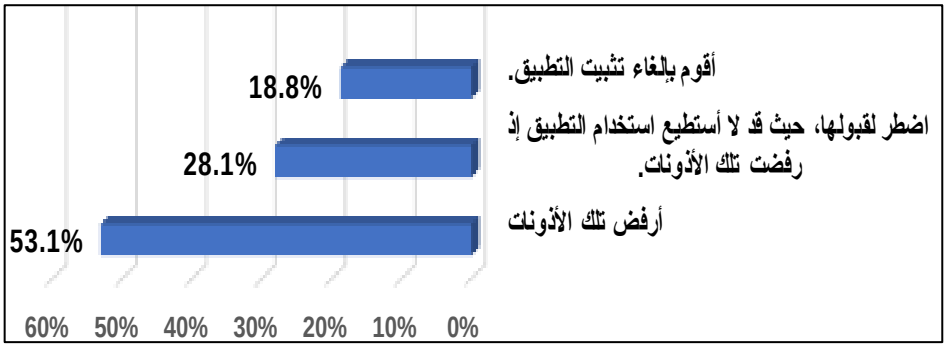
شكل رقم (٩): مستوى فهم مستخدمي تطبيقات الصحة المتنقلة لسياسات الخصوصية لتلك التطبيقات

ولقد توجهت الباحثة بسؤال إلى مستخدمي تطبيقات الصحة المتنقلة من أفراد العينة ما إذا كانوا يهتموا بمراجعة الاذونات التي تطلبها تطبيقات الصحة المتنقلة للوصول لبيانات معينة على هواتفهم، وقد جاءت إجاباتهم كما هو موضح بالشكل رقم(١٠) حيث أفاد(٤٢) مشارك بنسبة (٤٥,٢٪) بأنهم لا يهتموا بذلك، بينما صرح (٣٢) مشارك بنسبة (٣٤,٤٪) بأنهم يهتمون بذلك، في حين أفاد (١٩) مشارك بنسبة (٢٠,٤٪) بأنهم لا يعرفون ما هذه الأذونات.



شكل رقم (١٠): اهتمام أفراد العينة بمراجعة الأذونات التي تطلبها تطبيقات الصحة المتنقلة

وعن الإجراء الذي يتخذه مستخدمي تطبيقات الصحة المتنقلة الذين يهتموا بمراجعة الأذونات التي تطلبها تلك التطبيقات(ن=٣٢) عندما يجدوا أن الأذونات التي يطلبها التطبيق مبالغ فيها، فكما هو موضح بالشكل رقم (١١)، فقد صرح (٥٣,١٪) بأنهم يقومون برفض تلك الأذونات، بينما أفاد (٢٨,١٪) بأنهم يضطرون لقبولها حيث لا يستطيعون استخدام التطبيق إذا رفضوها، إذا فهم ليس لديهم الرغبة في الاستغناء عن تلك التطبيقات رغم معرفتهم بأنها تسهم في انتهاك خصوصيتهم، وأشار (١٨,٨٪) بأنهم يقومون بإلغاء تثبيت التطبيق.



شكل رقم (١١): إجراءات أفراد العينة عند مراجعة الأذونات المبالغ فيها التي تطلبها التطبيقات

وعن الممارسات والآليات التي يحرص عليها أفراد العينة من مستخدمي تطبيقات الصحة المتنقلة (ن=٩٣) لإدارة وحماية خصوصيتهم، فقد جاءت استجابات أفراد العينة كما هو موضح في الجدول رقم (١٥).

جدول رقم (١٥): الممارسات التي يحرص عليها أفراد العينة لحماية وإدارة خصوصيتهم على تطبيقات الصحة المتنقلة

الممارسات التي يحرص عليها أفراد العينة لحماية وإدارة خصوصيتهم على تطبيقات الصحة المتنقلة	ن=٩٣								
	دائما		أحيانا		أبدا		المتوسط الحسابي	الترتيب	المستوى
	ك	النسبة ٪	ك	النسبة ٪	ك	النسبة ٪			
استخدم معلومات مزيفة أو وهمية للتسجيل على التطبيق	5	5.4%	34	36.6%	54	58.1%	0.24	11	ضعيف
استخدم برامج متخصصة لحماية خصوصية بياناتي الشخصية.	11	11.8%	36	38.7%	46	49.5%	0.31	8	ضعيف
استخدم شبكة خاصة افتراضية (VPN) أثناء استخدام تلك التطبيقات	1	1.1%	18	19.4%	74	79.6%	0.11	14	ضعيف
اهتم بمراجعة سياسات الخصوصية والاستغناء عن التطبيقات التي تتطلب الوصول لمعلومات شخصية أو صحية لا حاجة لهم بها			38	40.9%	55	59.1%	0.20	12	ضعيف
أتابع باستمرار إعدادات الخصوصية الخاصة بي على تلك التطبيقات			51	54.8%	42	45.2%	0.27	10	ضعيف
أتحقق من الأذونات التي تطلبها التطبيقات قبل تثبيتها	12	12.9%	37	39.8%	44	47.3%	0.33	7	ضعيف
أقوم بمراجعة الأذونات التي يحصل عليها كل تطبيق وأتحكم فيها بصفة مستمرة	9	9.7%	35	37.6%	49	52.7%	0.28	9	ضعيف
أهتم بحذف جميع ملفات تعريف الارتباط على هاتفي بصفة مستمرة			26	28.0%	67	72.0%	0.14	13	ضعيف
أقوم بإيقاف وصول التطبيقات لموقعي الجغرافي أو تقييد وصولها بأن تكون وقت استخدام التطبيق فقط	5	5.4%	55	59.1%	33	35.5%	0.35	6	متوسط
استخدم كلمات مرور قوية للتطبيق من الصعب تخمينها.	74	79.6%	19	20.4%			0.90	1	عال
اهتم بالإطلاع على مراجعات المستخدمين لتقييم التطبيق فقد أجد بها تعليقات أمنية	١٣	14.0%	43	46.2%	37	39.8%	0.37	4	متوسط
اهتم بمعرفة معلومات عن سمعة الشركة المطورة للتطبيق			67	72.0%	26	28.0%	0.36	5	متوسط
اهتم بتثبيت برامج مضادة للفيروسات على هاتفي لفحص التطبيقات بعد تثبيتها	41	44.1%	32	34.4%	20	21.5%	0.61	3	متوسط
اهتم بإلغاء وحذف التطبيقات التي لم أعد استخدمها	63	67.7%	18	19.4%	12	12.9%	0.77	2	عال
المتوسط الحسابي العام	0.38								متوسط

يلاحظ من جدول رقم (١٥) أن درجة ممارسة مستخدمي تطبيقات الصحة المتنقلة عينة الدراسة لآليات الحماية جاءت متوسطة، إذ بلغ المتوسط الحسابي(٠,٣٨)، مما يعني أن هناك حاجة لمزيد من الجهود للتوعية بآليات حماية الخصوصية وإجراءات الأمان اللازمة لحماية البيانات لمستخدمي الهواتف الذكية بصفة عامة ومستخدمي تطبيقات الصحة المتنقلة بصفة خاصة.

وتكشف نتائج الجدول رقم (١٥) أن المتوسطات الحسابية لممارسات وآليات حماية الخصوصية التي يتبعها أفراد العينة من مستخدمو تطبيقات الصحة المتنقلة تراوحت ما بين (٠,٩٠) و (٠,١١)، وبالنظر إلى أعلى المتوسطات يتضح أن هناك عبارتان فقط حصلتا على درجة ممارسة عالية من مستخدمي تطبيقات الصحة المتنقلة عينة الدراسة، فقد جاءت عبارة " استخدم كلمة مرور قوية يصعب تخمينها" أكثر ممارسات وآليات حماية الخصوصية لدى أفراد العينة بمتوسط حسابي بلغ (٠,٩٠) وهذا من شأنه تعزيز وحماية حساب المستخدم من محاولات الاختراق.

وقد جاء "اهتم بإلغاء وحذف التطبيقات التي لم أعد استخدمها" في المرتبة الثانية بالنسبة لممارسات وآليات الحماية بمتوسط حسابي بلغ (٠,٧٧)، وهو ما يمكن اعتباره مؤشرا جيدا، فمن الضروري أن يقوم المستخدم بحذف التطبيقات غير المستخدمة على هاتفه الذكي لما لها من مخاطر على خصوصية البيانات،

لأن استمرار وجودها وتثبيتها على الهاتف يعني أنها مازالت تجمع الكثير من البيانات عن المستخدم بل قد تحاول الوصول إلى بيانات لا علاقة لها بوظيفتها.

كما حصلت أربع عبارات فقط على درجة ممارسة "متوسطة" من أفراد العينة، تبدأ بعبارة "اهتم بتثبيت برامج مضادة للفيروسات على هاتفي لفحص التطبيقات بعد تثبيتها" بمتوسط حسابي بلغ (٠,٦١) وهذا من شأنه حماية بيانات المستخدم وهاتفه من برامج التجسس و البرامج الضارة التي يمكنها الوصول إلى أجزاء الهاتف بدون إذن المستخدم، يليها عبارة "اهتم بالاطلاع على مراجعات المستخدمين لتقييم التطبيق فقد أجد بها تعليقات أمنية" بمتوسط حسابي بلغ (٠,٣٧) فقد يسهم ذلك في التأكد من سلامة التطبيقات قبل التحميل بناءً على آراء مستخدمين آخرين، وفي المرتبة الخامسة "اهتم بمعرفة معلومات عن الشركة المطورة للتطبيق" بمتوسط حسابي بلغ (٠,٣٦)، تلا ذلك عبارة" أقوم بإيقاف وصول التطبيقات لموقعي الجغرافي أو تقييد وصولها بأن تكون وقت استخدام التطبيق فقط" بمتوسط حسابي بلغ (٠,٣٥). ويدل ذلك على عدم وعي المستخدمين أن تحديد موقع المستخدم يُعد من طرق انتهاك الخصوصية.

كما حققت ثماني عبارات أدنى المتوسطات الحسابية لتكون بذلك درجة ممارسة أفراد العينة من مستخدمي تطبيقات الصحة المتنقلة لها "ضعيفة"، تبدأ بعبارة ""أتحقق من الأذونات التي تطلبها التطبيقات قبل تثبيتها" بمتوسط حسابي (٠,٣٣) فلابد أن يقوم المستخدم بمراجعة الاذونات التي تطلبها التطبيقات قبل تثبيتها لتحديد ما إذا كان التطبيق موثوقا أم لا وهل حقا يحتاج هذه الأذونات، يليها عبارة "استخدم برامج متخصصة لحماية خصوصية بياناتي" بمتوسط حسابي بلغ (٠,٣١).

وحققت عبارة " أقوم بمراجعة الأذونات التي يحصل عليها كل تطبيق واتحكم فيها بصفة مستمرة" المرتبة التاسعة بمتوسط حسابي بلغ (٠,٢٨)، تلا ذلك عبارة" أتابع باستمرار إعدادات الخصوصية الخاصة بي على تلك التطبيقات" بمتوسط حسابي بلغ (٠,٢٧) وتبرز أهمية هذا الإجراء في كونه يساعد المستخدم على تأمين حسابه عن طريق ضبط إعدادات الخصوصية على التطبيق لتحديد نطاق الخصوصية، وفي المرتبة الحادية عشر جاءت عبارة" استخدم معلومات مزيفة أو وهمية للتسجيل على التطبيق" بمتوسط حسابي بلغ (٠,٢٤)، يليها عبارة " اهتم بمراجعة سياسة الخصوصية والاستغناء عن التطبيقات التي تتطلب الوصول لمعلومات شخصية أو صحية لا حاجة لهم بها" بمتوسط حسابي بلغ (٠,٢٠) وهو متوسط ضعيف للغاية لا يتناسب مع أهمية صفحات سياسات الخصوصية فإن حماية خصوصية المستخدم تتطلب الاطلاع على بنود الخصوصية بشكل دوري، حيث أن هذه البنود قابلة للتغيير والتحديث بشكل مستمر.

وجاءت عبارة "اهتم بحذف جميع ملفات تعريف الارتباط على هاتفي بصفة مستمرة" في المرتبة الثالثة عشر بمتوسط حسابي بلغ (٠,١٤)، وأخيرا في المرتبة الأخيرة جاءت عبارة" "استخدم شبكة خاصة افتراضية VPN عند استخدام تلك التطبيقات" بمتوسط حسابي بلغ (٠,١١) لكل منهما.

وبناءً على ما سبق يتضح أن غالبية أفراد العينة من مستخدمي تطبيقات الصحة المتنقلة يفتقدون الوعي بالخصوصية، فقد تبين أن انشغالهم بقضية الخصوصية كان نظريا فقط، ولكنهم أقل اهتماما بها من حيث التطبيق العملي، والذي يتضح من انخفاض مستوى ممارساتهم لإدارة وحماية خصوصيتهم، رغم ما كشف عنه غالبية أفراد العينة من أن الخصوصية بالنسبة لهم كانت مهمة جدا.

رابعا: نتائج الدراسة:

تستعرض الباحثة هنا أهم النتائج التي توصلت إليها الدراسة مع محاولة مقارنتها مع نتائج الدراسات السابقة:

١/٤ نتائج الدراسة التحليلية لسياسات الخصوصية لتطبيقات الصحة المتنقلة عينة الدراسة:

توصلت الباحثة من خلال الدراسة التحليلية لمحتوى سياسات الخصوصية لتطبيقات الصحة المتنقلة عينة الدراسة إلى عدد من النتائج، وفيما يلي عرض لأهم النتائج التي تم التوصل إليها.

- تبين من الدراسة أن مستوى امتثال مقدمو الخدمة بتطبيقات الصحة المتنقلة عينة الدراسة للوائح وقوانين الخصوصية ومدى التزامهم بالكشف عن ممارساتهم حيال خصوصية المستخدمين كان ضعيفا بمتوسط حسابي بلغ (٠,٣٢). وتتفق هذه النتيجة مع دراسة (Bachiri, Idri, Fernández-Alemán & Toval, 2018) والتي أظهرت أن جميع سياسات الخصوصية التي تم تحليلها لا تتوافق تماما مع لوائح الخصوصية، كما تتفق مع دراسة Savla & Martino (٢٠١٢) والتي توصلت نتائجها إلى أن امتثال سياسات الخصوصية لمبادئ FID كان ضعيفا. وتختلف هذه النتيجة مع دراسة Alhomod & Shafi(٢٠١٢) والتي توصلت إلى أن ٦٠٪ من المواقع الحكومية السعودية التي لديها سياسة خصوصية تتوافق سياستها مع مبادئ الاستخدام العادل للمعلومات.

- تضمنت جميع تطبيقات الصحة المتنقلة عينة الدراسة ماعدا تطبيق واحد فقط سياسة للخصوصية، وتختلف هذه النتيجة مع كل من دراسة Sunyaev, Dehling, Taylor, & Mandl, 2015) والتي أظهرت نتائجها أن ٣٠,٥٪ فقط من التطبيقات لديها سياسات خصوصية، ودراسة Alhomod & Shafi(٢٠١٢) والتي توصلت إلى أن ٢٨٪ فقط من المواقع لديها سياسة خصوصية على موقعها، ودراسة Savla & Martino (٢٠١٢) والتي توصلت إلى أن ٩٪ من المواقع لم تتضمن سياسة خصوصية، كما تختلف أيضًا مع نتائج دراسة الخثعمي(٢٠١٧) والتي توصلت إلى أن نسبة ٥٢٪ فقط من إجمالي المواقع الالكترونية للجامعات الحكومية السعودية توفر سياسة خصوصية.

- وفقا للمقياس الذي وضعته الدراسة تم تصنيف نسبة (٣٩,٩٪) من التطبيقات على أنها ذات مخاطر خصوصية مرتفعة، بينما صُنفت نسبة (٣٤,٦٪) بأنها ذات مخاطر خصوصية مرتفعة جدا، وتتفق هذه النتيجة مع دراسة (Benjumea, et al., 2020) والتي توصلت إلى أن ٣٩٪ من التطبيقات حصلوا على أقل من ٥٠ درجة من أصل ١٠٠ في مقياس الامتثال للوائح وقوانين الخصوصية. بينما تختلف هذه النتيجة مع دراسة (Njie, 2018) والتي توصلت إلى أن ٢٨٪ من التطبيقات تنطوي على مخاطر منخفضة للخصوصية.

- ركزت التطبيقات عينة الدراسة إلى حد ما في سياساتها على الكشف عن أغراض جمع وتحليل البيانات وممارسات مشاركة البيانات مع أطراف ثالثة، تلا ذلك حق المستخدم وسيطرته على بياناته، في حين أغفلت غالبية تطبيقات الصحة المتنقلة عينة الدراسة في سياساتها الكشف عن ممارسات تأمين بيانات المستخدمين، والإبلاغ عن تحديث أو تعديل سياسة الخصوصية والإبلاغ عن تسريب البيانات.

- اهتمت غالبية التطبيقات عينة الدراسة بنسبة (٦٦,٧٪) بتوافر بند خاص بالخصوصية للأطفال، وتختلف هذه النتيجة مع دراسة كل من المتبولي (٢٠٢٢) والتي توصلت إلى إغفال معظم

المكتبات عينة الدراسة لعنصر خصوصية التعامل مع الأطفال، كما تختلف مع دراسة (أحمد، ٢٠٠٩) والتي توصلت إلى أن غالبية محركات البحث العربية قد تجاهلت موقفها من خصوصية الأطفال.

- جاءت سياسات الخصوصية لـ (٧٨) تطبيق بنسبة (٥١٪) غير واضحة وغير قابلة للفهم من قبل المستخدم العادي. وتتفق النتيجة مع دراسة (Sunyaev, Dehling, Taylor, & Mandl, 2015) والتي توصلت إلى أن غالبية ممارسات الخصوصية لتطبيقات الصحة المتنقلة غير واضحة وغير مفهومة للمستخدمين حيث يتطلب فهمها مستوى عالي من التعليم.
- أهمل (١١٦) تطبيق بنسبة (٧٥,٨٪) نهائيا تعريف المصطلحات التقنية والقانونية المستخدمة في سياسة الخصوصية.
- لم يلتزم (٦٩) تطبيق بنسبة (٤٥,١٪) بإعلام المستخدم بأنواع البيانات التي تجمعها ملفات تعريف الارتباط مطلقا، وتختلف هذه النتيجة مع دراسة (المتبولي، ٢٠٢٢) والتي توصلت إلى أن غالبية المكتبات الوطنية والجامعية الأجنبية عينة الدراسة اهتمت بذكر أنواع البيانات التي تُجمع بجانب من التفصيل.
- لم يطلب (٩٣) تطبيق بنسبة (٦٠,٨٪) موافقة المستخدم الصريحة لبدء تخزين وجمع بيانات صحة المستخدم والبيانات الحساسة عند إنشاء الحساب.
- لم يلتزم (١٣٥) تطبيق بنسبة (٨٨,٢٪) بالكشف عن مدة الاحتفاظ بالبيانات التي تجمعها ملفات تعريف الارتباط. وتتفق هذه النتيجة مع دراسة (أحمد، ٢٠٠٩) والتي توصلت إلى أن غالبية سياسات الخصوصية في محركات البحث عينة الدراسة لم تذكر فترة الاحتفاظ بالمعلومات.
- كشفت النتائج أن تطبيقات الصحة المتنقلة عينة الدراسة تجمع بيانات تفصيلية عن المستخدمين، وقد جاء الاسم والبريد الالكتروني على رأس البيانات الشخصية التي تطلبها التطبيقات حيث تم طلبهما في نسبة (٨١٪) من التطبيقات، كما يجمع (٧٤) تطبيق بنسبة (٤٨,٤٪) معلومات عن الموقع الجغرافي، وتتفق النتيجة مع دراسة (Zimmeck, et al., 2016) والتي توصلت إلى أن ٤١٪ من التطبيقات تجمع معلومات عن الموقع الجغرافي.
- طلبت نسبة قليلة من التطبيقات بيانات ترى الباحثة أنها تتجاوز الغرض الأساسي المحدد الذي تُجمع البيانات من أجله كعنوان المنزل والمهنة ورقم بطاقة الهوية الشخصية ورقم جواز السفر.
- تطلب تطبيقات الصحة المتنقلة عدد كبير من الأذونات. وقد تبين من تحليل الأذونات التي تطلبها التطبيقات عينة الدراسة أن هناك أذونات ضرورية وقد تحتاج إليها التطبيقات بالفعل لأداء مهمتها، ولكن هناك أيضا أذونات غير ضرورية وغير مبررة. كإذن الوصول إلى الموقع والذي تم طلبه في (٢٨,١٪) من التطبيقات، وإذن الوصول إلى جهات الاتصال والذي تم طلبه في (١٥٪) من التطبيقات، وإذن الوصول لسجل المكالمات والذي تم طلبه في (٦,٥٪) من التطبيقات، وإذن الوصول إلى مساحة التخزين في (٦٧,٣٪) من التطبيقات، وتتفق النتيجة مع دراسة Furini, Mirri, Montangero & Prandi(٢٠٢٠) والتي توصلت إلى أن ٢٤٪ من التطبيقات المثبتة بالفعل على أجهزة أفراد العينة تصل إلى جهات الاتصال و ٣٩٪ تنتهك خصوصية الموقع، و٥٦٪ لديها حق الوصول إلى الملفات والصور.
- كشفت نسبة (٢٣,٥٪) من التطبيقات عن أغراض جمع البيانات ولكن بصورة عامة وغير محددة، كما لم يمتثل (٣٣) تطبيق بنسبة (٢١,٦٪) للوائح وقوانين الخصوصية في الكشف

بوضوح عن أغراض جمع البيانات حيث لم يكشفوا في سياساتهم عن تلك الأغراض نهائيا. وتتفق النتيجة مع دراسة De & Shukla (٢٠٢٢) والتي توصلت إلى أن صياغة الغرض المحدد لجمع البيانات كان عام في غالبية السياسات.

- لم يفصح (١٩) تطبيق فقط بنسبة (١٢,٤٪) عن مشاركة المعلومات مع أطراف ثالثة، وتتفق النتيجة مع دراسة (Zimmeck, et al., 2016) والتي توصلت إلى أن ١٧٪ من التطبيقات تشارك المعلومات مع طرف ثالث دون أن يتم الإفصاح عن ذلك في سياسة الخصوصية، وتختلف هذه النتيجة مع دراسة (Apuru & Andembubtob & Audu Dodo, 2017) والتي توصلت إلى أن ٦٠٪ من التطبيقات لم تذكر بوضوح ما إذا كانت تشارك بيانات المستخدم مع أطراف ثالثة أم لا.
- لم يكشف (٦١) تطبيق بنسبة (٣٩,٩٪) عن الجهات الخارجية التي يشارك البيانات معها بشكل حصري.
- لم يطلب (١٢٩) تطبيق بنسبة (٨٤,٣٪) موافقة المستخدم الصريحة على مشاركة بياناته مع جهات خارجية. كما أخلت غالبية التطبيقات مسؤوليتها عن الأطراف الخارجية التي تتشارك بيانات المستخدم معها، وتتفق هذه النتيجة مع دراسة (أحمد، ٢٠٠٩) حيث أخلت ستة محركات بحث من إجمالي عشر محركات تمثل عينة الدراسة مسؤوليتها عن المواقع الأخرى.
- أغفل مطورو (٥١) تطبيق بنسبة (٣٣,٣٪) الإفصاح عن التدابير التي يتخذونها لحماية بيانات المستخدم.
- اعترف (٦١) تطبيق فقط بنسبة (٣٩,٩٪) بحق المستخدم في الغاء اشتراكه في التطبيق ويلتزم التطبيق بحذف بيانات المستخدم، وتختلف هذه النتيجة مع دراسة (Apuru & Andembubtob & Audu Dodo, 2017) والتي أظهرت أن أقل من ٢٣٪ من التطبيقات أظهرت آليات واضحة لإلغاء الاشتراك وحذف البيانات.
- لم يعرض (٨٠) تطبيق بنسبة (٥٢,٣٪) حق المستخدم في طلب محو بياناته نهائيا، كما لم يعرض (٩٢) تطبيق بنسبة (٦٠,١٪) حق المستخدم في طلب نسخة قابلة للقراءة ومنظمة من بياناته.

٢/٤ نتائج الدراسة الميدانية:

توصلت الباحثة من خلال الدراسة التي أجريت على عينة من المجتمع المصري للتعرف على واقع استخدام تطبيقات الصحة المتنقلة ورصد ممارسات مستخدموها لإدارة وحماية خصوصيتهم إلى مجموعة من النتائج، وفيما يلي عرض لأهم النتائج التي تم التوصل إليها.

- أشارت نسبة (٤٦,٢٪) من أفراد العينة بأنهم يستخدمون بالفعل تطبيقات الصحة المتنقلة على هواتفهم الذكية، وتتفق هذه النتيجة مع دراسة (Apuru & Andembubtob & Audu Dodo, 2017) والتي توصلت إلى أن ٤٦٪ من العينة قاموا بتحميل تطبيقات الصحة المتنقلة على هواتفهم.
- تفوقت المخاوف الصحية لأفراد العينة على مخاوف الخصوصية، بالنسبة لأسباب عدم استخدامهم لتطبيقات الصحة المتنقلة، كما أفادت نسبة (٣٢,٧٪) بأنهم لا يعلمون بوجود تطبيقات طبية وصحية على متاجر التطبيقات.
- جاءت تطبيقات الصحة المتنقلة المجانية في مقدمة التطبيقات التي يستخدمها أفراد العينة بنسبة (٦٦٪).

- أن النسبة الأكبر وهي (٤٦,٢٪) من إجمالي عينة الدراسة يستخدمون تطبيقات الصحة المتنقلة أسبوعيا، في حين أن (٢١,٥٪) يستخدمونها عند الحاجة فقط.
- فيما يتعلق بمدى أهمية الخصوصية الرقمية بالنسبة لمستخدمي تطبيقات الصحة المتنقلة عينة الدراسة، فقد أفادت نسبة (٥٩,١٪) بأنها مهمة جدا بالنسبة لهم، كما أفادت ما نسبته (٣٧,٦٪) بأنها متوسطة الأهمية.
- فيما يتعلق بمدى قلق أفراد العينة المستخدمين لتطبيقات الصحة المتنقلة من توافر معلوماتهم الشخصية والحساسة على تلك التطبيقات، فقد أفاد (٤٦,٢٪) من المستخدمين بأنهم قلقون إلى حد ما، بينما أفاد(٣٣,٣٪) بأنهم غير قلقون.
- عن مستوى ثقة مستخدمي تطبيقات الصحة المتنقلة من أفراد العينة في مستوى تأمين تلك التطبيقات لبياناتهم الشخصية والحساسة، فقد صرح (٥١٪) بأنهم لم يفكروا في الأمر من قبل.
- أفادت نسبة (٤٦,٢٪) بأنهم لم يقرأوا أبدا سياسات الخصوصية لتطبيقات الصحة المتنقلة قبل تثبيتها على هواتفهم المحمولة، وتتفق النتيجة مع دراسة (Lawler & Molluzzo, 2010) والتي أظهرت نتائجها أن ٥٥,٦٪ من المستجيبين لم يقرأوا سياسة الخصوصية لمواقع التواصل الاجتماعي. بينما تختلف النتيجة مع دراسة uru & Andembubtob & Audu Dodoa (٢٠١٧) والتي توصلت إلى أن ٥٩٪ من مستخدمي تطبيقات الصحة المتنقلة يقومون بقراءة سياسة الخصوصية لتلك التطبيقات.
- أفاد(٤٢) مشارك بنسبة (٤٥,٢٪) بأنهم لا يهتموا بمراجعة الأذونات التي تطلبها تطبيقات الصحة المتنقلة للوصول لبيانات معينة على هواتفهم، في حين أفاد (١٩) مشارك بنسبة (٢٠,٤٪) بأنهم لا يعرفون ما هذه الأذونات. وتختلف النتيجة مع دراسة (Ali, Rahman & Jahan, 2019) والتي توصلت إلى أن ١١,٦٪ فقط لم يقرأوا الأذونات التي يطلبها التطبيق قبل تثبيته على الهاتف، كما تختلف مع النتيجة التي توصلت إليها دراسة (Apuru & Andembubtob & Audu Dodo, 2017) من أن ٨٢٪ من أفراد العينة يأخذون الوقت الكافي لمراجعة الأذونات المطلوبة من قبل التطبيقات.
- عن الإجراء الذي يتخذه مستخدمي تطبيقات الصحة المتنقلة عينة الدراسة عندما يجدوا أن الأذونات التي يطلبها التطبيق مبالغ فيها، فقد صرح (٣٤,٧٪) بأنهم يقومون برفض تلك الأذونات، بينما أفاد (١٨,٤٪) بأنهم يضطرون لقبولها حيث لا يستطيعون استخدام التطبيق إذا رفضوها.
- جاءت درجة ممارسة مستخدمي تطبيقات الصحة المتنقلة عينة الدراسة لآليات الحماية متوسطة، إذ بلغ المتوسط الحسابي(٠,٣٨)، مما يعني أن هناك حاجة لمزيد من الجهود للتوعية بآليات حماية الخصوصية وإجراءات الأمان اللازمة لحماية البيانات لمستخدمي الهواتف الذكية بصفة عامة ومستخدمي تطبيقات الصحة المتنقلة بصفة خاصة، وتتفق النتيجة مع دراسة (Ali, Rahman & Jahan, 2019) والتي توصلت إلى أن أن ٦٠٪ من المستجيبين لا يدركون أمن الهواتف الذكية والخصوصية، كما تتفق مع دراسة (Albatat, Clar & Abulkhair, 2023) والتي توصلت إلى أن غالبية المستجيبين بنسبة ٧٢,٣٪ لديهم وعي متوسط بالخصوصية.
- جاءت عبارة "استخدم كلمة مرور قوية يصعب تخمينها" أكثر ممارسات وآليات حماية الخصوصية لدى أفراد العينة بمتوسط حسابي بلغ (٠,٩٠)، كما جاءت عبارة "اهتم بإلغاء وحذف

التطبيقات التي لم أعد استخدمها" في المرتبة الثانية بالنسبة لممارسات وآليات الحماية بمتوسط حسابي بلغ (٠,٧٧).

خامسًا: توصيات الدراسة:

من خلال نتائج الدراسة توصي الباحثة بعدد من التوصيات، من أهمها:

- الاهتمام بسن القوانين التي تضمن كافة الحقوق لمستخدمي تطبيقات الهواتف الذكية وتطبيقات الصحة المتنقلة بصفة خاصة لتقليل المخاطر التي تواجه مستخدمي تلك التطبيقات، والعمل على تحديثها ومراجعتها باستمرار لتتماشى مع التطورات في عالم التكنولوجيا.
- السعي نحو إقامة معاهدات دولية واتفاقيات تكون ملزمة لجميع الدول تضبط المعايير الخاصة بحق الخصوصية مع تطويرها باستمرار تماشيا مع العصر الرقمي.
- أن يتبنى مطورو تطبيقات الصحة المتنقلة أفضل الممارسات والمعايير للأمن والخصوصية نظرا لطبيعتها الخاصة كونها تتعامل مع بيانات المستخدمين الحساسة.
- العمل على نشر الوعي بين مطوري تطبيقات الهواتف الذكية بشأن ضرورة الامتثال لقوانين ولوائح حماية البيانات الشخصية والحساسة عند صياغة سياسات الخصوصية للتطبيقات الرقمية، مع توضيح العقوبات في حال انتهاك خصوصية المستخدمين.
- ضرورة أن يعمل مطورو التطبيقات والمواقع على الحد من الأذونات التي تنتهك الخصوصية والتي تطلبها التطبيقات.
- عمل حملات توعية لتثقيف المواطنين بشأن حقوقهم وواجباتهم تجاه خصوصيتهم الرقمية وطرق مواجهة انتهاكات الخصوصية، وتوعيتهم بوجود قانون لحماية البيانات الشخصية في مصر، لأن الرفع من وعي مستخدمي التطبيقات بالخصوصية من شأنه دفع مطوري التطبيقات على التعامل مع بيانات المستخدم بشكل أكثر مسؤولية.
- إدراج مقررا عن الثقافة الرقمية في المناهج الدراسية بمؤسسات التعليم المختلفة للتعريف بمخاطر التكنولوجيا والتوعية بكيفية التعامل الإيجابي مع التقنيات الحديثة للحفاظ على الخصوصية.
- نشر ثقافة الإبلاغ بين الأفراد في حالة حدوث أي انتهاك لخصوصيتهم.
- صياغة صفحات سياسات الخصوصية بشكل واضح وموجز دون أن يخل بالهدف منها حتى يتمكن جميع المستخدمين – على اختلاف مستوياتهم التعليمية – من فهمها، وتقترح الباحثة إتاحتها في ملف صوتي بحيث يستمع إليها المستخدم بدلا من قراءتها.
- إتاحة آليات للتعاون بين مطوري تطبيقات الصحة المتنقلة ومنظمة الصحة العالمية ومنظمات الخصوصية بشأن إقرار صياغة موحدة لسياسات الخصوصية لتطبيقات الصحة المتنقلة، مع ضرورة تفعيلها والالتزام بها.

المصادر:

أبو سريع، حسام الدين محمد رفعت (٢٠٢٠). تطبيقات الهواتف الذكية والخصوصية المعلوماتية: دراسة تحليلية مقارنة. *المجلة الدولية لعلوم المكتبات والمعلومات والأرشيف*، مج٧، ع٣، ١٨٠-٢٢٥.

أحمد، إبراهيم شاهين (٢٠١١). خصوصية المعلومات وسريتها بمواقع الحكومات الالكترونية العربية: دراسة مقارنة. *مجلة الاتجاهات الحديثة في المكتبات والمعلومات*، ع٣٥.

أحمد، فايزة دسوقي (٢٠٠٩). سياسات الخصوصية في محركات البحث: دراسة تحليلية مقارنة. *دراسات المعلومات*، ع ٥، ٤٩-٨٠.

أحمد، هندي عبد الله هندي (٢٠١٧). قانون حماية البيانات الشخصية في مواقع التواصل الاجتماعي لمؤسسات المكتبات والمعلومات: دراسة تحليل مضمون. في المؤتمر الثامن والعشرون: شبكات التواصل الاجتماعي وتأثيراتها في مؤسسات المعلومات في الوطن العربي.

الخثعمي، مها بنت دخيل الله (٢٠١٧). سياسة الخصوصية في مواقع الجامعات الحكومية السعودية على الانترنت: دراسة تحليلية. *مجلة دراسات، العلوم التربوية*، مج٤٤، ع٤، ٣٥٣: ٣٧٢.

المتبولي، هبة أحمد محمد (٢٠٢٢). سياسة حماية خصوصية بيانات المستفيدين من المكتبات في البيئة الرقمية: دراسة تحليلية على عينة من المكتبات الأجنبية مع استنباط سياسة للمكتبات العربية. *مجلة بحوث في علم المكتبات والمعلومات*، مج٢٩، ع٢٩، ١٧٣- ٢١٦.

النشار، غادة صلاح الدين (٢٠١٨). إدارة الخصوصية في مواقع التواصل الاجتماعي بالتطبيق على موقع فيسبوك "دراسة في المفهوم والممارسة". *المجلة العلمية لبحوث الإعلام والتليفزيون*، ع١٤، ٢٧٠-٣٣٥.

اليونسكو (٢٠١٣). دراسة استقصائية عالمية حول خصوصية الانترنت وحرية التعبير. متاح على https://unesdoc.unesco.org/ark:/48223/pf0000218273_ara

سليمان، ياسر رجب علي (٢٠٢١). مدى وعي أعضاء هيئة التدريس ومعاونيهم بجامعة جنوب الوادي بسياسة الخصوصية في مواقع التواصل الاجتماعي وتأثيره على التشارك المعرفي: دراسة ميدانية. *مجلة كلية الآداب –جامعة بنها*، ع.٥٦، ٢-٦٨.

عبد الرحمن، دعاء حامد محمد (٢٠٢٢). الموافقة ودورها في تقنين التعامل في البيانات الصحية والحساسة وتأثيرها على الأمن المعلوماتي: قراءة في قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠. *مجلة الدراسات القانونية والاقتصادية*، مج٨. ١-٤٩.

عبد الله، خالد سالم (٢٠١٩). الخصوصية في عصر الإنترنت ومواقع التواصل الاجتماعي. *مجلة كلية التربية*، ع.١٦، ١١٧- ١٤٩.

قاسم، حشمت (٢٠١٣). الحماية القانونية للخصوصية. في المؤتمر العلمي العاشر لقسم المكتبات والوثائق وتقنية المعلومات. كلية الآداب. جامعة القاهرة.

كدواني، شيرين محمد (٢٠٢٢). ضوابط حماية الحق في الخصوصية عبر مواقع التواصل الاجتماعي: دراسة تحليلية. *مجلة البحوث الإعلامية*، ع٦٠، ج٢، ٩٠٣: ٩٤٨

مؤمنة، اعتماد محمد صالح (٢٠٢٢). تقييم استخدام التطبيقات الصحية لمرتادي العيادات الخارجية ومراكز الرعاية الصحية الأولية في مدينة الرياض. *مجلة دراسات المعلومات والتكنولوجي*، مج٢(١٢).

محكمة النقض المصرية (٢٠٢٠). القانون رقم ١٥١ لسنة ٢٠٢٠ https://www.cc.gov.eg/legislation_single?id=404869

مصطفى، بن قارة (٢٠١٦). الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية. *مجلة البحوث القانونية والسياسية*، ع٦، ٢٧٢-٢٨٩.

مكاوي، محمد حسن عماد (٢٠٢٢). الخصوصية الرقمية في القانون الدولي والمواثيق الدولية. *مجلة البحوث والدراسات الإعلامية*، ع٢٠، ١- ٧٤.

يس، إيمان عبد الحميد؛ السيد، أماني (٢٠٢٢). الخصوصية وحماية البيانات الشخصية بالمكتبات: مراجعة علمية. *المجلة الدولية لعلوم المكتبات والمعلومات*. مج٩، ع٢، ٤٧٧- ٤٩٣.

Affonso, E. P., & Sant'Ana, R. C. G. (2018). Privacy awareness issues in user data collection by digital libraries. *IFLA journal*, 44(3), 170-182

Alhomod, S. M., & Shafi, M. M. (2012). Privacy policy in e government Websites: A case study of Saudi Arabia. *Computer and Information Science*, 5(2), 88

Ali, M. N. Y., Rahman, M. L., & Jahan, I. (2019). Security and privacy awareness: A survey for smartphone user. *Editorial Preface from the* Desk of Managing Editor, 10(9).

Apuru, Jonathan & Andembubtob, David & Audu Dodo, Kafwa. (2017). User Awareness of Privacy Concerns Posed by the Use of mHealth Apps. *International Journal of Engineering and Computer Science*, 6. 22486-22497. 10.18535/ijecs/v6i9.16.

Avuglah, B. K., Owusu-Ansah, C. M., Tachie-Donkor, G., & Yeboah, E. B. (2020). Privacy issues in libraries with online services: attitudes and concerns of academic librarians and university students in Ghana. *College & Research Libraries*, 81(6), 997.

Bachiri, M., Idri, A., Fernández-Alemán, J. L., & Toval, A. (2018). Evaluating the privacy policies of mobile personal health records for pregnancy monitoring. *Journal of medical systems*, 42, 1-14

Bailey, J. (2018). Data protection in UK library and information services: are we ready for GDPR?. *Legal information management*, 18(1), 28-34.

Benjumea, J., Ropero, J., Rivera-Romero, O., Dorronzoro-Zubiete, E., & Carrasco, A. (2020). Assessment of the fairness of privacy policies of mobile health apps: scale development and evaluation in cancer apps. *JMIR mHealth and uHealth*, 8(7), e17134

Bowers, J., Reaves, B., Sherman, I. N., Traynor, P., & Butler, K. (2017). Regulators, mount up! analysis of privacy policies for mobile money services. In Thirteenth symposium on usable privacy and security (SOUPS 2017) (pp. 97-114).

Chan, J. (2021). Exploring digital health care: eHealth, mHealth, and librarian opportunities. Journal of the Medical Library Association: *JMLA*, 109(3), 376.

Chen, Hsuan-Ting. (2018). Revisiting the Privacy Paradox on Social Media with an Extended Privacy Calculus Model: The Effect of Privacy Concerns, Privacy Self-Efficacy, and Social Capital on Privacy Management. *American Behavioral Scientist*. 62. 1392-1412. 10.1177/0002764218792691.

De, S. J., & Shukla, R. (2022). An analysis of privacy policies of public COVID-19 apps: Evidence from India. *Journal of Public Affairs*, 22, e2801.

Furini, M., Mirri, S., Montangero, M., & Prandi, C. (2020). Privacy perception when using smartphone applications. *Mobile Networks and Applications*, 25, 1055-1061.

Havelka, S. (2021). Typologies of mobile privacy behavior and attitude: a case study comparing German and American library and information science students. *The Serials Librarian*, 81(1), 42-58

Huckvale, K., Torous, J., & Larsen, M. E. (2019). Assessment of the data sharing and privacy practices of smartphone apps for depression and smoking cessation. *JAMA network open*, 2(4), e192542-e192542.

Katulić, A. (2023). Information privacy culture in Croatian libraries*. Library Management*. https://www.emerald.com/insight/content/doi/10.1108/LM-03-2023-0020/full/html

Kritikos, K. C., & Zimmer, M. (2017). Privacy policies and practices with cloud-based services in public libraries: An exploratory case of bibliocommons. *Journal of Intellectual Freedom & Privacy*, 2(1), 23-37.

Lambert, A. D., Parker, M., & Bashir, M. (2015). Library patron privacy in jeopardy an analysis of the privacy policies of digital content vendors. *Proceedings of the Association for Information Science and Technology*, 52(1), 1-9

Lane, N. D., Miluzzo, E., Lu, H., Peebles, D., Choudhury, T., & Campbell, A. T. (2010). A survey of mobile phone sensing. *IEEE Communications magazine*, 48(9), 140-150

Lawler, J. P., & Molluzzo, J. C. (2010). A study of the perceptions of students on privacy and security on social networking sites (SNS) on the internet. *Journal of Information Systems Applied Research*, 3(12), 3-18

Liu, J., Sun, H. L., & Zheng, J. (2023). Factors affecting users' intention to use mobile health services of public libraries. *Library & Information Science Research*, 45(1), 101223.

McKinnon, D., & Turp, C. (2022). Are library vendors doing enough to protect users? A content analysis of major ILS privacy policies. *The Journal of Academic Librarianship*, 48(2), 102505

Moscato, D. R., Altschuller, S., & Moscato, E. D. (2013). Privacy policies on global banks' websites: does culture matter? *Communications of the international information management association*, 13(4), 7.

Njie, C. M. L. (2013)."Technical analysis of the data practices and privacy risks of 43 popular mobile health and fitness applications", 2013, [online] Available: https://www.privacyrights.org/

O'Brien, P., WH Young, S., Arlitsch, K., & Benedict, K. (2018). Protecting privacy on the web: A study of HTTPS and Google Analytics implementation in academic library websites. *Online Information Review*, 42(6), 734-751.

Papathanassopoulos, S., Athanasiadis, E., & Xenofontos, M. (2016). Athenian University Students on Facebook and Privacy: A Fair "Trade-Off"? *Social Media+ Society*, 2(3), 2056305116662171

Pitkänen, O., & Tuunainen, V. K. (2012). Disclosing personal data socially—An empirical study on Facebook users' privacy awareness. *Journal of Information Privacy and Security*, 8(1), 3-29.

Reitz, Joan M. (2014). Online Dictionary for Library and Information Science. https://odlis.abc-clio.com/odlis_p.html

Shahid, A., & Abdullah, U. (2020). Privacy threats on social networking websites. *Foundation University Journal of Engineering and Applied Sciences* (HEC Recognized Y Category, ISSN 2706-7351), 1(1).

Sunyaev, A., Dehling, T., Taylor, P. L., & Mandl, K. D. (2015). Availability and quality of mobile health app privacy policies. *Journal of the American Medical Informatics Association*, 22(e1), e28-e33

Tummon, N., & McKinnon, D. (2018). Attitudes and practices of Canadian academic librarians regarding library and online privacy: A national study*. Library & Information Science Research*, 40(2), 86-97.

World Health Organization (2011). mHealth: new horizons for health through mobile technologies: second global survey on eHealth Available from: https://apps.who.int/iris/handle/10665/44607.

Yerukhimovich, A., Balebako, R., Boustead, A.E., Cunningham, R.K., Welser, W., Housley, R., Shay, R., Spensky, C., Stanley, K.D., Stewart, J., Trachtenberg, A., & Winkelman, Z. (2016). Can Smartphones and Privacy Coexist Assessing Technologies and Regulations Protecting Personal Data on Android and iOS Devices. https://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1393/RAND_RR1393.pdf

Zimmeck, S., Wang, Z., Zou, L., Iyengar, R., Liu, B., Schaub, F., ... & Reidenberg, J. (2016, September). Automated analysis of privacy requirements for mobile apps. In 2016 AAAI Fall Symposium Series.

Savla, P., & Martino, L. D. (2012, July). Content analysis of privacy policies for health social networks. *In 2012 IEEE International Symposium on Policies for Distributed Systems and Networks* (pp. 94-101). IEEE

Huuskonen, P., Häkkilä, J., & Cheverst, K. (2015, August). Who needs a doctor anymore? risks and promise of mobile health apps. *In Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services Adjunc*t (pp. 870-872).

Albatati, H. A., Clark, J. A., & Abulkhair, M. F. (2023, July). Privacy Awareness Among Users of Digital Healthcare Services in Saudi Arabia. *In International Conference on Human-Computer Interaction* (pp. 247-261). Cham: Springer Nature Switzerland.