العوامل المؤثرة على مخاوف الخصوصية لمستخدمى روبوت الدردشة ودورها فى التجنب السلوكى والإفصاح عن المعلومات [1]

د. نرمين أحمد عبد المنعم السعدنى

الأستاذ المساعد بقسم إدارة الأعمال

كلية التجارة - جامعة القاهرة

جمهورية مصر العربية

nermeenelsadany@foc.cu.edu.eg

ملخص البحث

تهدف الدراسة إلى تقديم إطار شامل للعوامل المؤثرة على شعور العملاء بمخاوف الخصوصية من استخدام روبوت الدردشة في الخدمة البنكية، وتأثير تلك المخاوف على التجنب السلوكي والإفصاح عن المعلومات.

تم جمع البيانات باستخدام قائمة استقصاء، وتوزيعها على عينة منتظمة بلغت (365) عميل من عملاء البنوك العاملة في مصر التى تقدم تلك الخدمة. أظهرت النتائج التي تم الحصول عليها باستخدام اسلوب نمذجة المعادلات الهيكلية، دعماً لمعظم فروض الدراسة. على وجه التحديد، كان هناك تأثير إيجابي لكل من القلق التكنولوجى، الألفة مع روبوت الدردشة، التحكم فى المعلومات، حساسية المعلومات، توافرالتشريعات والقوانين الحكومية، الأدوات التكنولوجية لدعم الخصوصية، الحاجة للتفاعل البشرى على مخاوف الخصوصية. بينما لم يظهر تأثير للرعاية الأخلاقية التنظيمية للخصوصية على مخاوف الخصوصية. كما أثرت مخاوف الخصوصية تأثيراً إيجابياً على التجنب السلوكي، وسلبياً على الإفصاح عن المعلومات.

الكلمات الدالة

القلق التكنولوجى - الألفة مع روبوت الدردشة - التحكم فى المعلومات - حساسية المعلومات -الرعاية الأخلاقية التنظيمية للخصوصية - مخاوف الخصوصية - التجنب السلوكى - الإفصاح عن المعلومات.

[1] تم تقديم البحث في 2024/5/7، وتم قبوله للنشر في 2024/6/5.

(1) المقدمة

لقد أتاحت الثورة الصناعية الرابعة، التى تُعرف أيضاً بالصناعة 4.0، أفاقاً جديدة من الإبداع والتنمية في جميع القطاعات الاقتصادية (Paul, Maglaras, Ferrag & Almomani, 2023)، وأثار الذكاء الاصطناعى اهتماماً واسعاً بفضل فوائده الواعدة (Hu & Min, 2023)، واستخداماته المتنوعة فى العديد من الأجهزة مثل أجهزة الإستشعار، وتمييز الصوت، التعلم الذكي، والروبوت (Fan, Lu & Mao, 2022). ويُعد روبوت الدردشة أو ما يطلق عليه الشات بوت "Chatbot" من الأدوات التى أحدثت تغيير بالغ الأثر في خدمة العملاء، والتى استُخدمت بدلاً من وكلاء خدمات الدردشة البشرية في العديد من المجالات، كما أنه من المتوقع أن تقود أكثر من 90٪ من محادثات خدمة العملاء عبر الإنترنت بحلول عام 2025 (Maduku, Mpinganjira, Rana, Thusi, Ledikwe & Mkhize, 2023).

ويعترف الباحثون والممارسون على نطاق واسع بالمزايا الاجتماعية والاقتصادية لاستخدام روبوتات الدردشة، بما في ذلك زيادة الكفاءة، وتخفيض التكاليف والأخطاء البشرية، وتعزيز خدمة العملاء (Chong, Yu, Keeling & de Ruyter, 2021)، كما يمكنها مساعدة العملاء في التخطيط للسفر، وحجز الفنادق، والتسوق (Balakrishnan & Dwivedi, 2021). ويمكنها أيضاً خدمة العديد من العملاء في نفس الوقت دون الحاجة إلى الانتظار لفترات طويلة، وتقديمها دعم فوري وفعال. وذلك لامتلاكها قدرة هائلة على جمع وتخزين معلومات عن العملاء واحتياجاتهم بشكل حصرى، مما يساعد في تحسين تجربة المستخدم باستمرار مقارنة بالوكلاء البشريين (Maduku et al., 2023).

بالإضافة إلى تفاعلها مع العملاء بلغتهم الطبيعية عبر الرسائل النصية أو الصوتية، كما تعفيهم من المهام المتكررة نسبياً، وتساعدهم في التعامل مع الطلب المتزايد، وتقديم الخدمات الترفيهية، وتنويع الخدمات وفقاً لطلب العملاء بناءً على ملفاتهم الشخصية (Hsu & Lin, 2023).

وبالرغم من المزايا السابقة إلا أن تلك التكنولوجيا أدت إلى ظهور العديد من التحديات المتعلقة بالأمن السيبراني، فقد أدى الانتشار الكبير لجمع وتحليل المعلومات الشخصية إلى زيادة مخاوف العملاء بشأن خصوصيتهم (Paul et al., 2023). وذلك لأن معلوماتهم الشخصية، وسلوكهم، وأنشطتهم عبر الإنترنت غالباً ما يتم تتبعها وتحليلها تلقائياً دون علمهم أو موافقتهم (Hong, Chan & Thong, 2021). كما يمكن استخدام وتوزيع هذه المعلومات بطرق غير مصرح بها، مما يعرضهم لخطر الانتهاكات الأمنية (Davenport, Guha, Grewal & Bressgott, 2020). نتيجة لذلك يشعر العملاء بأنهم تحت المراقبة، مما يثير مخاوفهم بشأن الخصوصية (Hu & Min, 2023).

وقد يتسبب الخوف المتزايد بشأن الخصوصية إلى دفع العملاء لاتخاذ تغييرات جذرية في سلوكهم، مثل إغلاق حساباتهم، أو تخفيض مشاركة معلوماتهم الشخصية، وتخفيض عمليات الشراء عبر الإنترنت. لذا من الضرورى دراسة العوامل الدافعة لشعور العملاء بمخاوف الخصوصية المتعلقة باستخدام روبوت الدردشة من أجل تصميم الاستراتيجيات المناسبة للحد من تلك المخاوف، ولتعزيز الثقة بين المنظمات وعملائها (Mattison Thompson & Siamagka, 2022; Hong et al., 2021).

ومع ذلك، تناولت دراسات قليلة العوامل التى قد تؤثرعلى مخاوف الخصوصية من استخدام روبوت الدردشة منها، سهولة الاستخدام(Chung, Ko, Joung & Kim, 2020; Sanny, Susastra, Roberts & Yusramdaleni, 2020)، التجسيد (Blut, Wang, Wünderlich & Brock, 2021)، عوامل الرضا (Ischen, Araujo, Voorveld, Van & Smi, 2020; Ng, Coopamootoo, Toreini, Aitken, Elliot & Van, 2020).

كما تناولت الدراسات السابقة استخدام روبوت الدردشة في عدة قطاعات، منها التأمين (Bouhia, Rajaobelina, PromTep, Arc & Ricard, 2022)، الاتصالات (Alashoor, Han & Joseph, 2017)، الرعاية الصحية (Paul et al., 2023).

فى حين لم يحظى القطاع المصرفى بالأهمية الكافية، على الرغم من تعرض بنوك كبيرة مثل Capital One في عام 2019، لانتهاك خطير للبيانات، باختراق أنظمته، وتسريب معلومات شخصية لنحو 106 مليون عميل. ونتيجة لذلك اتخذت البنوك خطوات محكمة لحماية خصوصية المعلومات، بما في ذلك تأكيد عدم نقل سجلات معاملات العملاء للمجال العام، والالتزام بسياسة الخصوصية لعدم الكشف عن معلوماتهم السرية (Neto, Madnick, Paula & Malara Borges, 2021).

وبالرجوع للدراسات السابقة يتضح أنها توصلت لنتائج متناقضة ومجزأة وغير متكاملة، ولا يزال هناك حاجة إلى إطار عمل متكامل لفهم أفضل للعوامل المؤثرة على مخاوف خصوصية العملاء في التفاعل مع روبوت الدردشة خاصة فى القطاع المالى. ولكن يظل تحديد الأسباب الحقيقية لمخاوف الخصوصية أمراً بعيد المنال، بسبب تداخل العديد من العوامل الخارجية والداخلية (Hu & Min, 2023). لذلك، أصبح فهم العوامل المؤثرة على شعور العملاء بمخاوف الخصوصية عند استخدام روبوت الدردشة فى الخدمة البنكية أمراً مُلحاً علمياً وعملياً.

وفى ظل وجود مخاوف للعملاء تتعلق بالخصوصية، والتى قد تكون عائقاً محتملا يساهم في مقاومة الأشخاص لاستخدام تكنولوجيا الذكاء الاصطناعى، إلا أن العديد منهم يُظهِر القليل من الاهتمام لحماية بياناتهم، وغالباً ما ينتهي بهم الأمر للكشف عن بياناتهم الشخصية، ويعرف هذا التناقض بمفارقة خصوصية المعلومات "Information Privacy Paradox" (Rodríguez-Priego, Porcu, Pena & Almendros, 2023). فعندما يُطلب من العملاء مشاركة بياناتهم الشخصية، فإن إدراكهم للمخاطر سيؤدي في أغلب الأحيان إلى رفض هذا الإحتمال. ولكن عندما يتعلق الأمر بتبادل تسويقي رقمي يعتمد على مشاركة البيانات الشخصية، لا يظهر الأفراد أي اتساق فى السلوك، مما يعني أنه غالباً ما يتم الكشف عن بياناتهم الشخصية (Gouthier, Nennstiel, Kern & Wendel, 2022). يشير ذلك إلى أن مزايا الكشف عن المعلومات الحساسة يمكن ملاحظتها بسهولة على المدى القصير، وتكون المخاطر المرتبطة بها غير واضحة أو مؤجلة على المدى الطويل. وقد يترتب على ذلك، نتائج غير حاسمة في الاستجابة السلوكية، مثل الإفصاح عن المعلومات أو رفض الكشف عنها أو تشويهها Distortion (Rodríguez-Priego et al.,2023). وهذا أمر محير، دفع الباحثة إلى معرفة السبب الجذري الذي يفسر النتائج المتضاربة لسلوك العملاء الناشئ من مخاوف الخصوصية عند استخدام روبوت الدردشة، والذى يتراوح بين الإفصاح عن المعلومات والتجنب السلوكى.

ولا تعتمد مخاوف الخصوصية لدى العملاء على عوامل فردية فقط مثل التجربة السابقة لإنتهاك الخصوصية (Ioannou, Tussyadiah & Lu, 2020)، والتحكم المدرك في الخصوصية (Morimoto, 2021). بل تعتمد أيضاً على عوامل أخرى مثل أنواع المعلومات الشخصية، التي يطلبها مقدمو الخدمة عبر الإنترنت، وحساسية المعلومات (Harborth & Pape, 2021; Jozani, Ayaburi, Ko & Choo, 2020).

وقد تبنى فريق من الدراسات نظريات مختلفة ترتبط بمخاوف الخصوصية مثل نظرية "التنمية متعددة الأبعاد" (MDT) Multidimensional Development Theory، التى قدمها كل من Laufer & Wolfe (1977)، والتى تنص على أن مخاوف الخصوصية تتأثر بأربعة عوامل هى: العوامل البيئية، والفردية، وإدارة المعلومات، وإدارة التفاعل (Hong et al., 2021). كما تبنى فريق آخر نموذج "المسببات - مخاوف الخصوصية – النتائج" Antecedents - Privacy Concerns - Outcomes (APCO)، الذى قدمه كل من (Smith, Dinev & Xu 2011) . وفقاً لهذا النموذج يقترح الباحثون أن مخاوف الخصوصية تمثل متغير يتوسط العلاقة بين العديد من المسببات والنتائج (Zhang & Zhang, 2024; Alashoor et al., 2017).

بالنظر إلى ما تم ذكره، يتضح مدى ملاءمة نظرية "التنمية متعددة الأبعاد" (MDT)، ونموذج "المسببات - مخاوف الخصوصية – النتائج" (APCO)، لموضوع الدراسة، مما دفع الباحثة إلى دمجهما معاً في نموذج واحد يخدم الدراسة الحالية، التى تأتي تلبية لدعوة العديد من الدراسات التي تطالب باستكشاف أسباب مخاوف الخصوصية عند استخدام

روبوتات الدردشة في الدول النامية والناشئة، وذلك بسبب الإختلافات الثقافية التى تؤثر على إدراك الأفراد بشأن الخصوصية، والتي تؤدي أيضاً إلى ظهور مستويات متفاوتة من المخاوف (Bouhia et al., 2022; Hong et al., 2021; Mogaji, Balakrishnan, Nwoba & Nguyen, 2021).

تسعى الدراسة الحالية من خلال التحليل الشامل لأسباب مخاوف الخصوصية ونتائجها السلوكية، إلى تقديم توجيهات مفيدة لممارسي الخدمة البنكية، ومصممي أنظمة الذكاء الاصطناعى لإدارة قضايا الخصوصية وتخفيف المخاطر المحتملة. كما يمكن مساعدة العملاء أيضاً في اتخاذ قرارات مبنية على وعي كامل بخصوصيتهم أثناء تفاعلهم مع روبوتات الدردشة.

بناءً على ذلك، تهدف هذه الدراسة إلى معرفة العوامل المؤثرة على شعور العملاء بمخاوف الخصوصية عند استخدام روبوت الدردشة فى الخدمة البنكية، ونتائجها السلوكية التى تتراوح ما بين الإفصاح عن المعلومات والتجنب السلوكى. تنقسم الدراسة إلى أربعة أقسام تشمل الدراسة الاستكشافية والمشكلة التي تتناولها الدراسة، ثم الإطار النظري الذي يتبعه مراجعة للدراسات السابقة، وتطوير فروض الدراسة، ثم المنهجية المتبعة في الدراسة، يليها تحليل البيانات ومناقشة النتائج، وأخيراً، تقديم التوصيات وتوضيح حدود الدراسة، ومقترحات للدراسات المستقبلية.

(2) الدراسة الاستكشافية

لفهم أفضل للعوامل المؤثرة على مخاوف الخصوصية لدى عملاء البنوك العاملة في مصر، والتي تقدم هذه الخدمة. تم إجراء مقابلات متعمقة شبه مهيكلة مع 23 عميل من العملاء المستهدفين، تم اختيارهم باستخدام طريقة العينة الميسرة. وكان متوسط مدة المقابلات نصف ساعة تقريباً، تم مناقشة هدف البحث بشكل واضح مع المشاركين، وطُلب منهم توضيح ما إذا كانوا قد استخدموا تطبيق روبوت الدردشة خلال الستة أشهر السابقة لتاريخ المقابلة أم لا؟. بناءً على ردهم على هذا السؤال، تم تحديد إجراءات المقابلة، حيث قام البعض بتفصيل تجربتهم مع روبوت الدردشة، بينما احتاج آخرون إلى المساعدة من خلال التعرف على شكل روبوت الدردشة لعدم معرفتهم بالإسم العلمي للتطبيق.

تم طرح أسئلة مثل: "هل تستخدم روبوت واحد فقط أم عدة روبوتات للعديد من البنوك؟"، "ما هي الأسباب وراء استخدام الروبوت؟"، و"ما هي أسباب تجنبه وعدم استخدامه؟". وللتحقيق في بعض النتائج المتناقضة في الدراسات السابقة، تم اختيار مجموعة من الموضوعات التي تم النظر فيها بعناية لإدراجها في هذه الدراسة كما هو موضح في جدول (1). تم تسجيل إجابات المستجيبين خلال المقابلة. ثم عرض صورة مرئية لاحقاً، لروبوت الدردشة الذى يحمل اسماً وشكلاً شبيهاً بالإنسان، يطلق عليه "إلينا"، لمعرفة رأي العملاء في تشبيه روبوتات الدردشة بالبشر.

جدول 1: آراء العملاء حول استخدام روبوتات الدردشة فى الخدمة البنكية

متغيرات الدراسة	الإجابات
مخاوف الخصوصية	- لا أكشف عن اسمى عند استخدام روبوت الدردشة، خوفاً من سرقة البيانات. - من الصعب توقع مخاطر روبوت الدردشة لأن الخطر يكمن في الاستخدام غير السليم لهذه البيانات. - لن يستخدم البنك معلوماتى الشخصية ضدى، ولكن هذه البيانات قد تتسرب من قاعدة بيانات البنك، وقد يقوم شخص ما بانتهاك هذه البيانات. - انا غير متأكد من أن هذه البيانات لن تستخدم إلا لهذا الغرض وليس لغيره. - أعتقد أننا نتجه أكثر فأكثر نحو انتهاك خصوصية العملاء. - أعتقد أن روبوتات الدردشة ستؤذينى، فقد يكون هناك احتمال للخطر. - لا يوجد مخاطرة، لا يمكن الوصول إلى حسابى، عندى ثقة شديدة فى البنك واستخدامه للتكنولوجيا الحديثة لراحتى وليس لإلحاق الضرر بى.

متغيرات الدراسة	الإجـابـات
الإفصاح عن المعلومات	- يجب أن أكشف عن بياناتى، وإلا لن أتمكن من الحصول على الخدمة. - ليس لدى خيار، ولابد من الكشف عن المعلومات. - لماذا يحتاجون إلى اسمى، لماذا لا أكتب أسماء وهمية.
التجنب	- عدم استخدام روبوت الدردشة هو أفضل حماية. - أفكر في تقليل استخدامي لروبوت الدردشة إذا شعرت بأن بياناتي ليست آمنة بشكل كافٍ. - تجنب استخدام روبوت الدردشة يزيد من حماية خصوصيتي، لأن بياناتى لن تتعرض للتحليل أو الاستخدام في أغراض أخرى دون موافقة صريحة منى.
حساسية المعلومات	- يعتمد الأمر على نوعية البيانات التي اكشف عنها، ومدى حساسيتها وعلى مدى خصوصية هذه البيانات. - أعتقد أن البنوك يجب أن تقدم خيارات للعملاء بشأن كمية ونوعية البيانات التي يرغبون في مشاركتها مع الغير. - أنا أكثر حساسية لمشاركة بياناتى المالية مقارنةً بالبيانات الشخصية الآخرى.
الأدوات التكنولوجية لدعم الخصوصية	- لا تجدى الحماية باستخدام جدران الحماية ومضادات الفيروسات. - أرى أن البنوك تحتاج إلى زيادة فى أنظمة الأمان لديها لحماية بياناتى من الإختراقات المحتملة. - أشك في إمكانية تحقيق حماية كاملة للبيانات حتى مع الأنظمة المتقدمة.
الرعاية الأخلاقية التنظيمية للخصوصية	- أثق بأن البنوك تتبع معايير أخلاقية عالية في التعامل مع بياناتي الشخصية. - أخشى من أن بياناتي قد تتسرب بسبب إهمال البنك، مما يجعلني أشك في التزامهم بالأخلاقيات في حماية البيانات. - البنك يشارك في مبادرات توعية حول حماية البيانات، مما يعكس اهتمامه بالمسئولية الأخلاقية تجاه المجتمع والعملاء.
الألفة مع روبوت الدردشة	- أحببت روبوت الدردشة لأنه متاح على مدار الساعة، وتمكنت من الحصول على المساعدة مساء دون الحاجة للانتظار حتى الصباح. - في بعض الأحيان، يقدم الروبوت إجابات غير دقيقة أو غير مفيدة، مما يجعلني أشعر بالإحباط. - روبوت الدردشة سهل الاستخدام. - شعرت بالراحة في التعامل مع روبوت الدردشة لأنه يمكنني من الحصول على المعلومات أو حل المشكلات بسرعة وفعالية. - اتعامل مع أكثر من ربوت لعدة بنوك مختلفة. - تعرفت على روبوت الدردشة من إيصال الحساب الذي تم إصداره من جهاز الصراف الآلي (ATM)، حيث وجدت معلوماته مطبوعة على الايصال.
القوانين والتشريعات الحكومية	- أتوقع أن تكون هناك قوانين واضحة لحماية خصوصية المعلومات. - البنك هو المسئول وليس الدولة، لا يمكن للدولة أن تتدخل في كل شيء. - أعتقد أن الجميع مطالبون بالمسئولية. - يجب على الدولة حماية خصوصية البيانات.
التحكم فى المعلومات	- أفقد السيطرة على بياناتى الشخصية بمجرد التفاعل مع روبوت الدردشة. - أحتاج إلى ضمانات كافية للسيطرة على بياناتى الشخصية. - أعتقد أنه سيكون لدي القدرة على التحكم في من يرغب فى الوصول إلى أي معلومات شخصية قمت بمشاركتها مع روبوت الدردشة.

متغيرات الدراسة	الإجـابـات
الحاجة للتفاعل البشرى	- بالرغم من فوائد استخدام روبوتات الدردشة، إلا أنني أفضل التفاعل مع موظفين بشريين لضمان حماية بياناتي. - استخدام روبوتات الدردشة في الخدمة البنكية اختيار مريح وفعال، فهى توفر ردوداً سريعة ومعلومات دقيقة دون الحاجة إلى التفاعل مع العاملين. - أفضل روبوت الدردشة الشبيه بالإنسان مقارنة بالشبيه بالآلة. - أفضل التعامل مع الروبوت إلينا بدلاً من **banki chat** كما فى الشكل (1).  **شكل 1: ربوت الدردشة إلينا وروبوت الدردشة** banki chat

المصدر: من إعداد الباحثة بناءً على نتائج الدراسة الاستطلاعية

تعكس هذه الآراء مجموعة متنوعة من المخاوف بشأن استخدام روبوتات الدردشة، وتسلط الضوء على جوانب مختلفة تتعلق بالخصوصية والتفاعل مع التكنولوجيا. بذلك، تتراوح آراء العملاء بين القلق والخوف من انتهاك الخصوصية وسرقة البيانات، وبين الرغبة فى التجنب والكشف عن المعلومات، كما يرغب بعض العملاء في مزيد من الشفافية والخيارات لحماية بياناتهم، بينما يرى آخرون أن الفوائد تفوق المخاطر، إذا ما كانت هناك ضمانات كافية لحماية البيانات. كما يتضح تباين آراء العملاء بين الإيجابية والسلبية فى استخدام روبوت الدردشة في الخدمة البنكية بناءً على تجاربهم الشخصية.

(3) مشكلة الدراسة

يزداد تعقد حماية المعلومات الشخصية في بيئة الإنترنت، نتيجة للتقدم الكبير الذي أحرزته تكنولوجيا الذكاء الاصطناعى بما في ذلك روبوتات الدردشة. لما لها من إمكانيات متطورة فى جمع وتحليل وتخزين البيانات الضخمة Big data، والتى تتفاقم معها مخاوف العملاء بشأن خصوصية معلوماتهم (Gouthier et al., 2022). ويعكس الانتشار المتزايد لروبوتات الدردشة مدى الاهتمام بإيجاد حلول لوظائف الخطوط الأمامية لخدمة العملاء، والتى تتطلب التفاعل بين الإنسان والآلة خاصة في القطاع المالي (Salem, 2024; Mozafari, Weiger & Hammerschmidt, 2022). وقد أثبتت روبوتات الدردشة فعاليتها في المجالات المصرفية باعتبارها أحد أدوات تكنولوجيا التحول الرقمي التى تسهل التفاعل مع خدمة العملاء(Mogaji & Nguyen, 2022; Riedel, Mulcahy & Northey, 2022; Eren, 2021). كما تعتبر مصدراً للميزة التنافسية، وأداة مساعدة لتحسين جودة خدمة العملاء، وتوفير الوقت والتكاليف والدعم السريع، وتقديم الخدمة على مدار الساعة (Bouhia et al., 2022; Ling, Tussyadiah, Tuomi, Stienmetz & Ioannou, 2021).

بينما يدرك العملاء بشكل متزايد الفوائد التي تقدمها روبوتات الدردشة، فهم يعتبرونها أيضاً تهديداً محتملاً، خاصة مع فشل كثير من برامج الدردشة الآلية في تلبية توقعاتهم (Woźniak, Karolus, Lang, Eckerth, Schöning, Rogers & Niess, 2021; Rese, Ganster & Baier, 2020). وبناءً على طبيعة المعاملات الإلكترونية التي تتطلب مشاركة المعلومات الشخصية والمالية، فقد أصبحت مخاوف الخصوصية وحماية البيانات الشخصية حتمية، لا سيما بعد الانتهاكات الأخيرة لأمن البيانات (Mogaji & Nguyen, 2022)، من فقدان لحيازة المعلومات الشخصية، وسرقة الهوية، والقرصنة، واستخدام بيانات العملاء لأغراض غير مشروعة. وترتب على ذلك تعرض العملاء للإنتقادات الإجتماعية وتشويه سمعتهم، وشعورهم بمخاوف الخصوصية، وضعف ثقتهم، وعدم تقبلهم للذكاء الاصطناعى (Gouthier et al., 2022). ومع توقع سيادة روبوتات الدردشة في خدمة العملاء في السنوات المقبلة (Xu, Niu & Zhao, 2023). وفى ظل توقع زيادة حجم سوق روبوتات الدردشة العالمية من 5.4 مليار دولار أمريكي في عام 2023 إلى 15.5 مليار دولار أمريكي في عام 2028 بمعدل نمو 23.3% (Markets &

(Markets, 2024. فإنه من المتوقع زيادة مخاوف العملاء بشأن الخصوصية، وخلق تحديات مستقبلية أمام المنظمات للحفاظ على عملائها، مما يبرز أهمية إعطاء الأولوية لفهم العوامل التي تؤثر على شعور العملاء بمخاوف الخصوصية عند استخدام روبوتات الدردشة (Zhang & Zhang, 2024).

وعلى الرغم من مخاوف العملاء بشأن الخصوصية فى التعامل مع روبوتات الدردشة، إلا أنه قد ينتهي بهم الأمر لاحقاً للكشف عن معلوماتهم الشخصية، وينخرطون في سلوك الإفصاح عن المعلومات، التى قد تكون حساسة للغاية. وصف هذا السلوك المتناقض بمفارقة الخصوصية "Privacy Paradox"، الذى تم تناوله على نطاق واسع فى الدراسات السابقة (Rodríguez-Priego et al., 2023; Roozen, Raedts & Waetermans, 2022; Bleier, Goldfarb & Tucker, 2020). وبالنظر للخصوصية على أنها سلعة يتم تقييمها بناءً على العائد والتكلفة، يعيد العملاء النظر فى الكشف عن معلوماتهم الشخصية كإستجابة سلوكية غير نهائية لمخاوف الخصوصية (Kolotylo-Kulkarni, Xia & Dhillon, 2021)، نتيجة لدوافعهم المتضاربة بين الإقتراب من المتعة بالإنجذاب نحو حافز ما لتحقيق هدف معين، والتراجع عنه فى ذات الوقت لتجنب العواقب السلبية المحتملة، وذلك وفقاً لنظرية الإقتراب والتجنب "Approach-Avoidance Theory" (Stubenvoll, Binder, Noetzel, Hirsch & Matthes, 2022). ويتسبب ذلك فى نهاية الأمر لتوتر كبير، خاصةً إذا كانت الدوافع المتناقضة متساوية فى الشدة (Rodríguez-Priego et al., 2023). وبتطبيق هذه النظرية على مجال الذكاء الاصطناعي، يتبين أن العملاء يبحثون عن محتوى مفيد وممتع، ويتجنبون المعلومات التي قد تؤدي إلى نتائج سلبية، خاصةً عندما يطلب منهم الكشف عن معلوماتهم الشخصية(Kelly, Kerr & Drennan, 2020).

وبموجب هذا، وبناءً على الدمج بين نظرية "التنمية متعددة الأبعاد" (MDT)، ونموذج "المسببات - مخاوف الخصوصية – النتائج" (APCO) حول خصوصية المعلومات، تبحث هذه الدراسة في الربط بين العوامل المؤثرة فى مخاوف الخصوصية وسلوكيات التجنب والإفصاح عن المعلومات عند التفاعل مع روبوت الدردشة في الخدمة البنكية. ويمكن تلخيص مشكلة الدراسة فيما يلي:

"ما هي العوامل الرئيسية التي تُسبب شعور العملاء بمخاوف الخصوصية عند استخدام روبوت الدردشة في الخدمة البنكية، وما تأثيرها على استجابتهم السلوكية؟"

(4) أهداف الدراسة

فى ضوء التساؤل السابق تسعى الدراسة الحالية لتحقيق العديد من الأهداف كما يلى :

(4-1) تقييم مخاوف الخصوصية للعملاء عند استخدام روبوت الدردشة فى الخدمة البنكية.

(4-2) تحديد أثر العوامل الفردية، البيئية، التفاعلية، المعلوماتية على مخاوف الخصوصية للعملاء عند استخدام روبوت الدردشة فى الخدمة البنكية.

(4-3) تحديد الأهمية النسبية للعوامل المؤثرة على مخاوف الخصوصية للعملاء عند استخدام روبوت الدردشة فى الخدمة البنكية.

(4-4) تحديد أثر مخاوف الخصوصية لدى العملاء عند استخدام روبوت الدردشة فى الخدمة البنكية على التجنب السلوكى، والإفصاح عن المعلومات.

(4-5) التوصل لخطة عمل ارشادية لتنفيذ توصيات الدراسة، التى تفيد الجهات المعنية مثل البنوك والمنظمات العاملة فى مجال تكنولوجيا الذكاء الاصطناعى والأمن السيبرانى.

(5) أهمية الدراسة

(5-1) الأهمية النظرية

- الاهتمام المتزايد بمفهوم الخصوصية فى استخدام روبوتات الدردشة في الدراسات التسويقية الحديثة، واعتباره من الموضوعات البارزة فى عصر الثورة الصناعية الرابعة والبيانات الضخمة (Salem, 2024; Hu & Min, 2023; Haenlein, Huang & Kaplan, 2022).
- الربط بين مجموعة متنوعة من التخصصات مثل تكنولوجيا المعلومات، والتسويق ،والقانون، وعلم النفس، مما يسهم في فهم أفضل لدراسة روبوتات الدردشة من المنظور التسويقي، والتى غالباً ما يتم تناولها من زاوية علوم الكمبيوتر أو الهندسة (Meyer-Waarden et al., 2020)، كما يثرى البحث مجال سلوك العملاء، وتسويق الخدمات، والتسويق التفاعلي، للاستفادة من أدوات الذكاء الاصطناعي.
- يدمج نموذج الدراسة المقترح بين "نظرية التنمية متعددة الأبعاد" (MDT)، ونموذج "المسببات - مخاوف الخصوصية – النتائج" (APCO)، لاختبار تأثير العوامل البيئية، والفردية، والتفاعلية، والمعلوماتية على مخاوف الخصوصية بدلاً من الاكتفاء بعامل واحد فقط، والتغلب على قيود الاعتماد على العلاقة ذات العامل الواحد، وهي مشكلة شائعة في الدراسات التقليدية المتعلقة بالخصوصية (Zhang & Zhang, 2024).
- لم تستكشف أى دراسة فى حدود علم الباحث، العوامل المتباينة المؤثرة على مخاوف الخصوصية، سواء بتأثيرها السلبي مثل، توافر الأدوات التكنولوجية لدعم الخصوصية، والتحكم في المعلومات، وتوافر القوانين والتشريعات الحكومية. أو بتأثيرها الإيجابي مثل، الحساسية للمعلومات، والحاجة للتفاعل البشري، والقلق التكنولوجي. ويمثل هذا تغيراً ملحوظاً عن الأبحاث السابقة التي اعتمدت على المنظور الإيجابي فقط في التعامل مع تلك العوامل، والتي لم تأخذ بعين الاعتبار العوامل السلبية التي قد تؤثر على قرارات العملاء. كما يشمل ذلك أيضاً التنوع في النتائج السلوكية، سواء كانت الإيجابية مثل الإفصاح عن المعلومات، أو السلبية مثل التجنب السلوكي.
- تعد هذه الدراسة واحدة من المحاولات القليلة جداً لفهم العوامل المؤثرة على مخاوف الخصوصية التي لم تُدرس بشكل كافٍ، مع التركيز على مجموعة من المتغيرات التي لم تلقَ الكثير من الاهتمام في الدراسات التسويقية، مثل القلق التكنولوجي والحساسية للمعلومات. كما توسع الدراسة من تطبيق مفهوم الرعاية الأخلاقية التنظيمية للخصوصية الذى يسلط الضوء على الدوافع العاطفية بدلاً من الدوافع العقلانية في السلوك التنظيمي، ليشمل ليس فقط الشركة وموظفيها، بل أيضاً العملاء. مما يعد متغيراً جديداً في مجال سلوك المستهلك، من منظور آلية التعامل مع مخاوف خصوصية العملاء.

(5-2) الأهمية التطبيقية

يحمل هذا البحث آثاراً عملية كبيرة منها ما يلى:

التطبيق على القطاع المصرفي الذى يلعب دوراً بارزاً في جذب وتحفيز المدخرات المحلية والأجنبية، وتقديم الحماية المالية للعملاء والمستثمرين، وتوفير حالة من الاستقرار المالي التي تُعتبر أساسية لتحقيق النمو الاقتصادي المستدام (الهيئة العامة للاستعلامات، 2023).

- يُعد قطاع الخدمات البنكية من أكثر القطاعات تعرضاً لانتهاكات البيانات والتهديدات الأمنية، ومن الضرورى مساعدة المؤسسات المالية بشكل عام، والبنوك بشكل خاص، في تحديد المشكلات المحتملة المتعلقة بخصوصية البيانات والأمن

وزيادة الوعي بها (Boggavarapu, 2021)، كما أن إدراك خطر روبوتات الدردشة فى اقتحام الخصوصيه، يمكن أن يولد موقفاً مشبوهاً تجاه البنوك التي تقدم هذه الخدمة (Ng et al., 2020).

- تعمل تكنولوجيا الذكاء الاصطناعى وخاصة روبوتات الدردشة في التحول الرقمي للصناعة المصرفية، وتُحسن من أداء العاملين، كما تقدم لهم فرصاً تدريبية متخصصة ومستمرة، لضمان تلبية احتياجات العملاء بشكل فعال، مما ينعكس إيجابياً على أداء البنوك (Salem, 2024).
- توفر الدراسة إرشادات عملية لتوجيه المديرين في تصميم وتنفيذ برامج الدردشة الآلية، كوسيلة فعالة لزيادة الإفصاح عن المعلومات ومنع سلوك التجنب. يتم ذلك من خلال فهم تأثير العديد من العوامل على مخاوف الخصوصية عند استخدام روبوتات الدردشة في الخدمات البنكية. وبالتالي، يمكن تطوير استراتيجيات تواصل فعالة لتحفيز السلوك المرغوب، وذلك بالتحكم في مثل هذه العوامل ومعالجتها، وتخفيض مخاوف العملاء بشأن الخصوصية (Mattison Thompson & Siamagka, 2022).
- كشف العوائق الأساسية التي تحول دون استخدام روبوتات الدردشة والأسباب الكامنة وراء مخاوف الخصوصية لدى عملاء البنوك، من خلال التحليل العميق لاحتياجاتهم وتفضيلاتهم وسلوكهم الفعلى. وتقديم حلول استباقية لتحسين إجراءات الأمان والحماية، لضمان سلامة المعلومات الشخصية والمالية، وتعزيز الابتكار والتطوير في الخدمات التكنولوجية المصرفية، وتحقيق أعلى عائد على التكاليف المستثمرة. كما يسهم هذا التحليل في تحسين تجربة العملاء، وبناء علاقات أكثر تفاعلية وموثوقية معهم.
- التأكد من الدور المركزي الذي تلعبه مخاوف الخصوصية في التجنب السلوكي والإفصاح عن المعلومات. فيما يتعلق بالتجنب، تعتبر هذه المخاوف مدمرة حيث تعيق عملية التواصل مع العملاء، ويصعب توصيل الرسالة للعملاء الذين يتجنبون التفاعل، بالإضافة إلى صعوبة إقناعهم أو إعلامهم بالمعلومات الهامة. أما فيما يتعلق بالإفصاح، فإن تخفيض هذه المخاوف يساهم فى زيادة رغبة العملاء فى الكشف عن المعلومات، مما يساعد فى تخفيض التكاليف التي يتحملها البنك للحصول على المعلومات الضرورية لتقديم المزيد من الخدمات المبتكرة التى تناسب احتياجات العملاء.
- لم تقتصر الدراسة على تحديد تأثير العوامل البيئية الرسمية مثل توافر القوانين والتشريعات الحكومية، بل شملت أيضاً البيئة التنظيمية الداخلية غير الرسمية مثل الرعاية الأخلاقية البنكية للخصوصية. يساعد هذا التناول الشامل على تعميق المعرفة لتأثير العوامل غير الرسمية في البيئة التنظيمية الداخلية، بالإضافة إلى تأثير البيئة الخارجية الرسمية على مخاوف الخصوصية لدى العملاء.

(6) الإطار النظرى لمتغيرات الدراسة

(6-1) روبوتات الدردشة

تشكل روبوتات الدردشة التي تستخدم الذكاء الاصطناعي جزءاً أساسياً في عالم الإنترنت، وتهدف إلى التفاعل والتواصل مع الأفراد باستخدام اللغة الطبيعية (Adam, Wessel & Benlian, 2020). تم تصميم هذه الروبوتات لتقليد الحوار البشري بأقصى درجة ممكنة، سواء كان ذلك نصياً أو صوتياً(Ling et al., 2021). كما تهدف إلى فهم استفسارات العملاء والرد عليها تلقائياً باستخدام أساليب متعددة مثل اللغة الطبيعية المعالجة، والتعلم الآلي، وإدارة الحوار، وبرمجة التطبيقات (Landim et al., 2022; Nißen et al., 2022). وتعتمد روبوتات الدردشة فى ذلك على بيانات من مصادر متعددة مثل مواقع الويب، والبريد الإلكتروني، وقواعد البيانات، وواجهات برمجة التطبيقات، ووسائل التواصل الاجتماعي، وسجلات محادثات دعم العملاء. وتخزينها فى ذاكرة مدمجة في تصميم النموذج (Senadheera et al., 2024). تشتهر روبوتات الدردشة

باستخدامها الواسع في مختلف المجالات مثل خدمة العملاء(Aslam, 2023) ، التجارة الإلكترونية ,.Maduku et al) (2023، الرعاية الصحية (Zhu, Janssen, Wang & Liu, 2022)، التأمين (Rajaobelina et al., 2021). الخدمات المصرفية (Limakrisna & Moeins, 2024)، السياحة (Jha, Gupta & Mahajan, 2023)، التعليم ,Rudolph, Ismail & Popenici) (2024، إلى جانب القطاعات الأخرى مثل القطاعات الترفيهية، والحكومية، والعقارية، والقانونية (Luo, Lau, Li&Si, 2022). وتسعى العديد من الشركات لدمج روبوتات الدردشة فى خدمة العملاء للمساعدة في أداء العديد من المهام مثل إجراء المعاملات، تقديم خدمات متخصصة، الرد على الأسئلة الشائعة (Davenport et al., 2020). ولتحقيق ذلك، تقوم الشركات بجمع بيانات من عملائها - الذين ربما لا يكونوا على علم بجمعها - لتحسين جودة الخدمة، ولتحقيق مزيد من الرفاهية، وتوفير الوقت والتكلفة (Ling et al., 2021)، ولتحسين تجربة العملاء وتحقيق ميزة تنافسية (Thomaz, Salge, Karahanna & Hulland, 2020).

(2-6) روبوتات الدردشة فى القطاع المصرفى

أصبحت روبوتات الدردشة أصولاً لا تقدر بثمن، ويزداد استخدامها في القطاع المصرفى حالياً، حيث توفرمجموعة متعددة من الفوائد لتطوير الخدمات المالية (Biswas, Carson, Chung, Singh & Thomas, 2020) حيث تساهم فى تقليل تكاليف التشغيل من خلال الرد على الأسئلة الشائعة، والاستفسارات حول الأرصدة، والتحويلات النقدية، ودفع الفواتير والإبلاغ عن فقدان البطاقات، و إجراء المدفوعات، وتجديد شهادات الاستثمار، والتعامل مع عملية استرداد الأموال (Salem, 2024). إضافة إلى تقديمها على مدار الساعة، هذا التطور يُمكّن موظفي خدمة العملاء من التركيز على التحديات الأكثر تعقيداً، مما يحسن كفاءة العمل ويطور الخدمات بشكل مستمر (Abdulquadri, Mogaji, Kieu & Nguyen, 2021). كما يُحسن من تجربة العملاء وذلك بتوفير تجربة مصرفية أكثر أماناً وفاعلية (Biswas et al., 2020).

بالإضافة إلى ذلك، تساعد روبوتات الدردشة المؤسسات المصرفية في جمع تعليقات العملاء والأفكار التي يمكن استخدامها لتطوير منتجات جديدة (Rani, Kanda, Chanchal & Vij, 2023).

ومع ذلك، لا تزال هناك شكوك حول قدرة روبوتات الدردشة على تحسين تجربة العميل في القطاع المصرفى (Jang, Jung & Kim, 2021; Sarbabidya & Saha, 2020)، وذلك بسبب مخاوف الخصوصية والأمان التي تشكل مصدر قلق للعملاء والبنوك على حدٍ سواء. وذلك لثقة العملاء في البنوك واعتقادهم بأن بياناتهم الشخصية لن يتم نشرها أبداً، ولكن قد يواجهون مخاوف بسبب حالات اختراق الأمان التي قد تؤدي إلى تسريب المعلومات. ولضمان حماية معلومات العملاء، وضعت البنوك سياسات الحماية واتخذت إجراءات هامة لعدم نقل سجلات المعاملات إلى جهات خارجية. كما التزمت البنوك بسياسات الخصوصية لحماية سرية المعلومات وعدم الكشف عنها، للحفاظ على ثقة عملائها (Rath & Kumar, 2021).

وعلى الرغم من وجود بعض الدراسات التي بحثت في اعتماد العملاء على تكنولوجيا مصرفية مماثلة مثل أجهزة الصراف الآلي والخدمات المصرفية عبر الإنترنت (Baklouti & Boukamcha, 2023; Coskun, Saygili & Karahan, 2022). إلا أن نتائج هذه الدراسات لم تكن قابلة للتعميم على روبوتات الدردشة المدعومة بالذكاء الاصطناعي، بسبب اختلاف دوافع وأنماط قبول روبوتات الدردشة المصرفية عن دوافع وأنماط قبول التكنولوجيا الأخرى (Salem, 2024). ولنجاح نشر روبوتات الدردشة في الخدمات المصرفية، يجب التركيز على معالجة مشاكل حماية خصوصية البيانات بعناية ومواجهة التحديات المتعلقة بفقدان التواصل البشري، من أجل ضمان توافر تجربة مستخدم مرضية وثقة عملاء مصرفية آمنة (Ngai, Lee, Luo, Chan & Liang, 2021; Satheesh, Samala & Rodriguez, 2020).

(3-6) مخاوف الخصوصية

استخدم مصطلح "الخصوصية" على نطاق واسع في العديد من الدراسات الإجتماعية والنفسية والقانونية والفلسفية، بالإضافة إلى مجال تكنولوجيا المعلومات، وتم ربطه بشكل أساسي بإدارة وحماية البيانات (Rodríguez-Priego et al., 2023). تُعرف الخصوصية بأنها "القدرة على حماية المعلومات الشخصية والحساسة من سوء الاستخدام" (Gouthier et al., 2022).

أما مخاوف الخصوصية Privacy Concerns يمكن تعريفها في مجال التسويق بأنها " قلق العملاء بشأن فقدان حقهم في حماية بياناتهم الشخصية وعدم القدرة على التحكم فيها" (Ischen et al., 2020)، كما تعكس معتقداتهم حول انتهاك الخصوصية عبر الإنترنت والمخاطر والعواقب السلبية المحتملة بعد جمع وتبادل المعلومات الشخصية (Aivazpour & Rao, 2019). وينتقد معارضو تكنولوجيا الوسائط الرقمية والمنتجات الذكية انتشارها وتطورها السريع، الذى يصاحبه زيادة فى مخاوف الخصوصية لدى العملاء والمستخدمين، وفقدهم السيطرة على معلوماتهم في بيئة الإنترنت بدرجة تفوق ما كانت عليه في البيئة التقليدية (Manikonda et al., 2018). من جهة أخرى، يرى مؤيدو التكنولوجيا الرقمية أن الخصوصية أصبحت جماعية وليست فردية، بمعنى أن البيانات الشخصية تُعتبر منظوراً جماعياً، فهم يرون أن البيانات الضخمة التي تُجمع من البيانات الشخصية ليست ملكية فردية بل يجب اعتبارها ملكية جماعية (Shaeffer & Keever, 2021).

بالرغم من الفوائد العديدة لروبوتات الدردشة، إلا أن المستخدمين يخشون إساءة استخدام معلوماتهم الشخصية في النظم القائمة على الذكاء الاصطناعي، والتي تعتمد بشكل كبير على البيانات الضخمة وعلى أطراف ثالثة لتحليلها وتخزينها (Lutz & Newlands, 2021). ومع التقدم في الذكاء الاصطناعي والتعلم الآلي، أصبح وكلاء المحادثة في شكل روبوتات الدردشة النصية أكثر أهمية بالنسبة للشركات والعلامات التجارية لتقديم توصيات قيمة متعلقة بالمنتج أو الخدمة (Følstad, Nordheim & Bjørkli, 2018).

تجمع الشركات التي تستخدم روبوتات الدردشة بيانات مستخدميها، الذين ربما لا يكونون على علم بذلك، مما يعزز مخاوف الخصوصية التي قد يواجهها المستخدمون عند التفاعل مع التكنولوجيا الرقمية (Ischen et al., 2020). وقد زادت مخاوف خصوصية المستخدمين نتيجة للكمية الكبيرة والأساليب المتنوعة لجمع البيانات المتاحة للأطراف المختلفة ليتم استغلالها بسهولة باستخدام أدوات متقدمة ورخيصة، كما أن الأجهزة التي تجمع وتولد هذه البيانات غالباً ما تكون غير مرئية للعملاء (Salem, 2024). ومع زيادة شعور المستخدمين بعدم اليقين والعجز بشأن التحكم في الكشف عن معلوماتهم الخاصة، فإنهم يضطرون إلى استخدام التكنولوجيا الذكية التى قد تبدو مخيفة، بالإضافة إلى مخاوفهم المتعلقة بالخصوصية (Rajaobelina et al., 2021). تأتي هذه المخاوف ضمن الجانب العاطفي المرتبط بمشاعر التهديد الناتج من جمع البيانات الشخصية وإساءة استخدامها، فالعملاء بحاجة إلى تزويدهم بخدمة آمنة عندما يتعلق الأمر بالتفاعلات مع برامج الدردشة الآلية (Ischen et al., 2020).

(4-6) العوامل المؤثرة على مخاوف الخصوصية

تم تسليط الضوء على عدة عوامل كمسببات لمخاوف الخصوصية التي يواجهها الأفراد عند استخدام تكنولوجيا الإنترنت، وذلك بالاعتماد على العديد من النظريات مثل نظرية "التنمية متعددة الأبعاد" (MDT) التي وضعها كل من Laufer &Wolfe (1977)، توفر هذه النظرية إطاراً قيماً يشرح متى ولماذا يُنظر إلى موقف معين على أنه تدخل في الخصوصية (Bartol, Prevodnik, Vehovar, & Petrovčič, 2022). وتقترح هذه النظرية أن إدراك الأفراد للتحكم فى معلوماتهم يعتمد على الشعور المتطور بالذات في التفاعل مع البيئة (Laufer & Wolfe, 1977). تتشكل مخاوف الخصوصية وفقاً لهذه النظرية من خلال

التفاعل بين عوامل متعددة تشمل العوامل البيئية، والفردية، وإدارة المعلومات، وإدارة التفاعل (Bartol et al., 2022; Hong et al., 2021).

كما يشير نموذج "المسببات - مخاوف الخصوصية – النتائج" (APCO) الذى وضعه Smith's et al. (2011)، إلى أن مخاوف الخصوصية من المرجح أن تتوسط العلاقة بين مجموعة من المسببات مثل تجربة الخصوصية، والوعي بالخصوصية، والشخصية، وبين النتائج السلوكية مثل الكشف عن الذات و التفاعل. يوفر نموذج (APCO) على المستوى الكلي إطاراً شاملا متعدد التخصصات، يساعد على معرفة الأسباب والنتائج المترتبة على مخاوف الخصوصية (Zhang & Zhang, 2024; Cheng, Qiao, Yang & Zhang, 2022). كما توجد ميزة أخرى مثيرة للاهتمام في نموذج (APCO) هي أنه يسمح بتوضيح التأثير المباشر وغير المباشر لمخاوف الخصوصية على قبول المستخدم للتكنولوجيا المرتبطة بالخصوصية (Strebinger & Treiblmaier, 2024).

تم استخدام نموذج (APCO) لتحليل المخاوف المتعلقة بالخصوصية لتكنولوجيا الدفع عن طريق التعرف على الوجه Facial Recognition Payment. كما تم تطبيقه في سياقات مختلفة مثل التجارة الإلكترونية (Bartol, Vehovar, Bosnjak & Petrov, 2023)، ووسائل التواصل الاجتماعى (Ozdemir, Smith & Benamati, 2018)، خدمات المستهلك المدعومة بتقنية البلوكشين Blockchain-Enabled Consumer Services (Strebinger & Treiblmaier, 2024). ويدل ذلك على قابلية النموذج العالية للتطبيق وتعدد استخداماته في القضايا المتعلقة بالخصوصية. وبناءً على ذلك، تدمج الدراسة الحالية كل من نظرية التنمية متعددة الأبعاد (MDT) ونموذج (APCO) كأساس نظري للدراسة.

(6-4-1) العوامل الفردية

يمثل البعد الفردى جوهر الخصوصية من حيث صلته بقدرة الفرد على إدارة معلوماته الشخصية في التفاعل مع الآخرين (Bartol et al., 2022)، تشمل العوامل الفردية والشخصية متغيرات مثل النوع، السن (Benamati, Ozdemir & Smith, 2016)، الخبرة التكنولوجية (Chen, Widarso & Sutrisno, 2020)، المخاطر المدركة (Jozani et al., 2020; Mutimukwe, Kolkowska & Grönlund, 2020)، الضعف المدرك، تجربة انتهاك الخصوصية، الشخصية، الثقافة والمعرفة (Adhikari & Panda., 2018).

تشير الأبحاث التي تناولت الأبعاد الفردية لمخاوف خصوصية العملاء، إلى أن الإحساس بالقلق التكنولوجى وانخفاض الألفة مع ربوت الدردشة يؤثران على استعداد العملاء لمشاركة معلوماتهم الشخصية. وبالتحكم في هذه العوامل يمكن للشركات تقليل مخاوف خصوصية عملائها وسلوكهم التخريبي، وزيادة مشاركة بياناتهم الشخصية (Zhang & Zhang, 2024; Bouhia et al., 2022). ومع ذلك، فقد كان هناك قلة فى الدراسات التي اهتمت بمسببات مخاوف الخصوصية فى استخدام روبوتات الدردشة. وبناء على نتائج الدراسة الاستطلاعية والدراسات السابقة تم اختيار متغيرين مرتبطين بالعوامل الفردية، وهما الألفة مع ربوت الدردشة، والقلق التكنولوجي. ويمكن توضيح كل منهما كما يلي:

(6-4-1-1) الألفة مع روبوت الدردشة

تعرف الألفة على أنها " المعرفة التى تعتمد على التفاعلات والتجارب السابقة للأفراد فيما يتعلق بما يفعلونه" (Gefen, 2000). فالألفة مع موقع الويب على سبيل المثال تشير إلى مدى معرفة المستخدم بالموقع الإلكتروني، بما في ذلك المعلومات المتعلقة بجمع البيانات واستخدامها، وطرق التحكم في الخصوصية، مما يؤثر على تقييم تجربة المستخدم وثقتة فى الموقع. إن زيادة المعرفة بموقع الويب يترتب عليها زيادة الألفة والمشاعر الإيجابية التي يشعر بها المستخدم، وتشجعه على استخدامه المستمر، والكشف الذاتي عن المعلومات الشخصية (Bouhia et al., 2022).

وبالمثل تعتمد الألفة مع روبوتات الدردشة على زيادة مستوى الخبرة والإلمام بها، وتفاعل المستخدمون معها، ويصبحون أكثر ألفة ووعياً بقدراتها (Mimoun, Poncin & Garnier, 2017). يتضمن التكيف مع روبوتات الدردشة فهم العملاء لكيفية استخدامها نتيجة لتجارب سابقة، والتى تيسر جميع التفاعلات المستقبلية وتؤثر على درجة تقييمهم لها (Pollmann, 2021).

كما تلعب مهارات المستخدمين دوراً هاماً فى رؤيتهم لروبوتات الدردشة على أنها أكثر فائدة وأقل استهلاكاً للوقت (Bekmanis, 2023)، إضافة إلى مستوى المعرفة والقراءة التى تزيد من درجة الارتباط بها، ويعتقد بعض المستخدمين الأكثر قراءة فى هذا المجال أن روبوتات الدردشة تكون أكثر كفاءة وإنتاجية. كما تُعتبر الخبرة المباشرة بالتجارب السابقة أكثر موثوقية مقارنة بالمعرفة الناتجة عن القراءة فقط. وبشكل عام كلما زاد الارتباط بروبوت الدردشة، زادت الثقة في هذا النظام. ومع تراكم الخبرة، يصبح المستخدمون أكثر إلماماً بالتكنولوجيا الحديثة، مما يسهل عليهم التفاعل معها (Mimoun et al., 2017).

(6-4-1-2) القلق التكنولوجى

يعتبر القلق التكنولوجى ظاهرة مرتبطة ارتباطاً وثيقاً بالسمات الشخصية، ويشير إلى تخوف المستخدمين من العواقب السلبية المحتملة المرتبطة باستخدام التكنولوجيا الحديثة (Zhang & Zhang, 2024). كما يعرف بأنه حالة عصبية وشعور بالإضطراب والتوتر تنتاب المستخدمين نتيجة للاستخدام والتفاعل مع الأجهزة التكنولوجية (Dogra, Adil, Sadiq, Rafiq & Paul, 2022).

تنشأ هذه المشاعر بسبب الإفتقار إلى الألفة، والصعوبة في تشغيل التكنولوجيا، فإذا شعر المستخدمون بالخوف من استخدام روبوت الدردشة، فإنهم يتجنبون التفاعل معه ويصبحون مقاومين لاستخدامه (Lee, Sheehan, Lee, Chang , 2021).

يمكن للقلق التكنولوجي أن يُضخم العبء النفسي للاستخدام القهري للتكنولوجيا وبالتالي، يُفترض أن التأثيرات المتراكمة للاستخدام القهرى للتكنولوجيا تساهم في التأثير السلبي على الرضا عن الحياة (Duong, Ngo, Khuc, Tran & Nguyen, 2024). بما فى ذلك استخدام ربوت الدردشة حيث يعد القلق التكنولوجى ميلاً نحو استجابات عاطفية سلبية لاستخدام التكنولوجيا، وعاملا رئيسيا في التنبؤ باستجابات المستخدمين السلوكية (Malodia, Kaur, Ractham, Sakashita, Dhir, 2022; Kim, Oh,Kim, 2021). ويتأثر مستوى القلق التكنولوجى بالعديد من العوامل مثل الخبرة، والعمر، والنوع، والكفاءة الذاتية (Kamal, Shafiq, Kakria, 2020; Tsai, Lin, Chang, Chang, Lee, 2020)، كما تؤدى المستويات العالية من القلق التكنولوجى إلى توتر المستخدمين، مما يخفض من احتمالية التفاعل، والإرتباط العاطفي والقدرة على نشر التعليقات الإيجابية عن روبوت الدردشة (Meng, Guo, Peng, Ye & Lai, 2022). وبالمثل، عندما يواجه المستخدمون مستويات أقل من القلق بشأن التكنولوجيا، فإنهم يشعرون بالثقة في استخدام روبوت الدردشة. وقد يشكل القلق التكنولوجي عائقا كبيرا قد يحول بين الرغبة في قبول التكنولوجيا الجديدة واستخدامها، ومع ذلك فإن فهم تأثير القلق التكنولوجي على سلوك المستهلكين يمثل تحدياً مهماً، يمكن أن يساهم في تطوير استراتيجيات للتغلب على هذا القلق وتعزيز قبول التكنولوجيا (Inan et al., 2022).

(6-4-2) العوامل المرتبطة بإدارة المعلومات

تعتبر إدارة المعلومات جزءاً حيوياً من تصميم وتطوير روبوتات الدردشة، وتهدف إلى ضمان سلامة وخصوصية المعلومات التي يتم تبادلها بين المستخدمين والروبوت (Bartol et al., 2022). تشير إدارة المعلومات إلى إدارة المستخدمين للمعلومات الشخصية، التي يتم إنشاؤها أثناء التفاعل مع الغير أو المنظمات من خلال الموازنة بين فوائد ومخاطر الكشف عن

المعلومات (Hong et al., 2021). وتتعلق إدارة المعلومات في المقام الأول بالعمليات العقلية التي ينخرط فيها الأفراد عند تحديد كمية المعلومات التي يجب الكشف عنها. وتقترح نظرية التنمية متعددة الأبعاد (MDT) أن المواقف التي يرى فيها الأفراد أن الكشف عن المعلومات قد يكون مفيداً، يكونوا أقل عرضة للحكم عليه باعتباره انتهاكاً للخصوصية (Laufer & Wolfe 1977). وهناك العديد من العوامل المؤثرة فى ادارة المعلومات منها حساسية المعلومات، التحكم فى المعلومات، ويمكن توضيح كل منهما كما يلى:

(6-2-4-1) حساسية المعلومات

تلعب حساسية المعلومات الشخصية دوراً محورياً في الكشف عن المعلومات (Sun, Zang, Wang, Zhao & Liu, 2023). فكلما كانت البيانات أكثرحساسية، زاد الخطر المدرك وانخفضت القيمة التى يتوقعها الأشخاص للكشف عن معلوماتهم الشخصية (Gouthier et al., 2022). تعرف حساسية المعلومات على أنها " سمة توضح مستوى الانزعاج الذي يشعر به الفرد عند الكشف عن معلوماته الشخصية لوكيل خارجي" فهى تعبر عن مستوى الاهتمام بالخصوصية الذي يشعر به الفرد تجاه نوع محدد من البيانات في موقف معين (Tao, Liu & Sun, 2024).

وتختلف حساسية المعلومات من شخص لآخر ومن حالة إلى أخرى، كما أن إدراك الأفراد لحساسية المعلومات يعتمد بشكل كبير على السياق المطلوب فيه الكشف عن المعلومات (Sun et al., 2023). بشكل عام، يظهر الأفراد مزيداً من الحذر في مشاركة معلوماتهم الشخصية ذات الحساسية العالية خوفاً من خطر تسريب هذه المعلومات والتعرض لمخاطر وخسائر محتملة (Degirmenci, 2020). كما يواجهون تقييمات معقدة للغاية فيما يتعلق بتكنولوجيا تحليل البيانات الضخمة، مما يجعلهم يشعرون بتحكم أقل في المعلومات التي يتم الكشف عنها أثناء تفاعلهم معها (Schomakers, Lidynia, Müllmann & Ziefle, 2019).

يمكن تقسيم المعلومات الشخصية إلى خمس فئات هى:

- المعلومات الحساسة للغاية والتى تشمل رقم جواز السفر والعنوان الحالي والحسابات البنكية ورقم الهاتف والبوم الصور.
- المعلومات الحساسة مثل سجل التسوق عبر الإنترنت، وتسجيل المكالمات والكاميرا.
- المعلومات المحايدة مثل الميكروفون والصوت وحالة الهاتف ومعلومات الموقع وجهات الاتصال وعنوان البريد الإلكتروني.
- المعلومات غير الحساسة مثل أجهزة استشعار الجسم لقياس مستوى النشاط البدنى، والعمر، والبلوتوث.
- المعلومات غير الحساسة للغاية مثل مستوى التعليم، والنوع، وأنواع الطعام المفضل (Sun et al., 2023).

(6-2-4-2) التحكم فى المعلومات

يعد التحكم في المعلومات الشخصية أمراً بالغ الأهمية لإدارة خصوصية المستخدم عبر الإنترنت. فالقدرة على منح أو سحب الإذن لمعالجة المعلومات الشخصية هي أمر أساسي للشعور بالخصوصية لدى مستخدمي الإنترنت (Tseng, Ibrahim, Hajli, Nisar & Shabbir, 2022).

ويلعب إدراك الأفراد لقدرتهم على التحكم في معلوماتهم الشخصية دوراً هاماً في إدارة خصوصيتهم ويؤثر بشكل كبير على سلوكهم عبر الإنترنت (Mattas, 2023).

ويُعتبر التحكم في المعلومات بمثابة بناء معرفي للحماية الذاتية للفرد، ويعبر عن اعتقاده في قدرته على التأثير في التغيرات التي قد تحدث في بيئة الإنترنت بطريقة مرغوبة (Lang, Wiesche, Krcmar, 2018). يُعرف التحكم فى المعلومات بأنه "اعتقاد

الفرد بوجود أدوات تؤثر في مدى قدرته على التحكم في معلوماته الشخصية" (Mattison Thompson & Siamagka, 2022).

تتعدد الأدوات التى يمكن أن يستخدمها الفرد للتحكم في معلوماته الشخصية عبر الإنترنت منها:

- تحديد الهوية، وذلك بتقديم معلومات موثوقة للتأكد من هوية المستخدم لضمان أن المعلومات المتبادلة تكون فقط مع الأطراف المعتمدة.
- أنظمة المصادقة، مثل كلمة المرور، الرمز المُرسل إلى الهاتف المحمول، التعرف على الوجه، وبصمات الأصابع.
- إجراءات الأمان، والتى تشمل تشفير البيانات، وتطبيق الإجراءات الوقائية مثل الجدران النارية وبرامج مكافحة الفيروسات، وتنفيذ تكنولوجيا التوثيق الثنائي والتوقيع الرقمي (Peltoniemi, 2020).
- إخفاء الهوية، حيث يتم استبدال معلومات التعريف الشخصى في سجل البيانات بتعريفات اصطناعية أو أسماء مستعارة، أو يتم دمج البيانات بطريقة تجعل من الصعب الوصول إلى البيانات الأصلية. تساعد هذه الإجراءات في حماية المعلومات من الوصول غير المصرح به وتقليل مخاطر انتهاكات الخصوصية (Mattas,2023).

يرغب الأفراد في التحكم في معلوماتهم الشخصية بسبب مخاوف تتعلق بالخصوصية والأمان. ويعزز التحكم المدرك للمعلومات الشخصية رغبة المستخدمين في مشاركة المزيد من المعلومات الخاصة عبر الإنترنت، خاصةً عندما يشعرون بقدرتهم على السيطرة على معلوماتهم (Wang & Liu, 2019). بينما قد يؤدي الشعور بفقدان السيطرة إلى اتخاذ مواقف سلبية تجاه مشاركة المعلومات أو إزالتها(Sheng et al., 2020).

وقد تناولت الدراسات السابقة التحكم فى المعلومات من جانبين مختلفين: الجانب السلوكي والجانب النفسي. يشير الجانب السلوكي إلى قدرة المستهلكين على التحكم في بياناتهم الشخصية، بينما يشير الجانب النفسي إلى تفكير المستهلكين وإدراكهم للتحكم في خصوصيتهم (Mattison Thompson & Siamagka, 2022). يمكن أيضاً التمييز بين نوعين من التحكم فى المعلومات: - التحكم في الكشف عن المعلومات - التحكم في استخدام المعلومات بمجرد الحصول عليها. عادةً ما يعالج مقدمو الخدمة عبر الإنترنت البعد الأول من خلال تقديم أدوات دقيقة تقيد إمكانية الوصول إلى المعلومات الحساسة للأعضاء والأطراف الأخرى (Lang et al., 2018).

(3-4-6) العوامل المرتبطة بالبيئة

يشمل البعد البيئي التفاعل بين البيئات الاجتماعية والتكنولوجية، والثقافية، والقانونية، والتنظيمية. تشكل هذه الجوانب وفقا لنظرية "التنمية متعددة الأبعاد"، توقعات الأفراد وادراكهم للخصوصية، كما توفر مبادئ معيارية للخصوصية مثل التشريعات والقوانين الصادرة من البيئة القانونية (Bartol et al., 2022)، وشفافية الشركة، وتخصيص الخدمات، إشعار الخصوصية، إضافة إلى الرعاية الأخلاقية التنظيمية للخصوصية فى البيئة التنظيمية، وذلك لحماية خصوصية المستخدمين عبر الإنترنت. إن الإلتزام بالبعد البيئى يساعد على تخفيض مخاوف الخصوصية لدى الأفراد (Schmidt, Bornschein & Maier, 2020). ويمكن توضيح الأبعاد البيئية بناء على الدراسات السابقة، ووفقاً لما أكدت عليه الدراسة الاستطلاعية فى الدراسة الحالية على النحو التالى:

(1-3-4-6) التشريعات والقوانين الحكومية لحماية الخصوصية

للتشريعات والقوانين الحكومية دوراً هاماً في تحقيق التوازن بين حقوق الأفراد ومتطلبات المنظمات الخاصة والعامة (Park, 2021. تشير قوانين حماية الخصوصية "إلى مجموعة القواعد واللوائح التي تنظم جمع واستخدام البيانات الشخصية على الإنترنت، وتوفر آليات يمكن للأفراد من خلالها المطالبة بحقوقهم في الخصوصية، كما تحد من سلطة المنظمات في جمع

واستخدام بياناتهم الشخصية" (Mattison Thompson & Siamagka, 2022). يرى فريق من الباحثين أهمية التشريعات والقوانين الحكومية في حماية خصوصية العملاء من الممارسات غير العادلة للشركات، التى تزيد من ثقتهم وتخفض من مخاوفهم وقلقهم (Acquisti, Brandimarte & Loewenstein, 2015).

فى حين يرى فريق آخر أن المنظمات عبر الإنترنت لديها دوافع لحماية خصوصية العملاء لتجنب فقدانهم بغض النظر عن القوانين المصدرة (Ginosar & Ariel, 2017). ومن القوانين التى تم اقرارها قانون حماية البيانات الشخصية رقم 151 لعام 2020 كخطوة قانونية هامة نحو ضمان أمان وسرية بيانات المواطنين، خاصةً مع غياب إطار قانوني ينظم حماية البيانات الشخصية التي يتم جمعها، وتخزينها، ومعالجتها الكترونياً (علي،2023)

وبقراءة سريعة لهذا القانون، يتضح أن المشرع المصري اتبع نهجين مختلفين لحماية البيانات الشخصية. فقد استثنى بعض البيانات الشخصية من الحماية التشريعية المعلوماتية مثل البيانات المستخدمة للأغراض الشخصية، تطبيق القانون، العمل القضائي، الأمن القومي، البيانات الإحصائية الرسمية (رجب،2022). وفي الوقت نفسه، فرض حماية مشددة على البيانات الحساسة، التي عرّفها في المادة الأولى ونظم أحكامها في المادة 12 من قانون حماية البيانات الشخصية، بحظر التعامل مع هذه البيانات إلا بعد الحصول على ترخيص وموافقة كتابية من الشخص المعني. تأتي هذه الحماية نتيجة لارتباط هذه البيانات بحريات الأفراد وخطر كشف هويتهم ونمط حياتهم، مما قد يهدد أمنهم وسلامتهم (عبد الرحمن، 2022).

إن عدم فعالية القوانين والتشريعات الحكومية تزيد من مخاوف الأفراد بشأن خصوصية بياناتهم (Anic, Budak, Rajh, Recher, Skare & Skrinjaric, 2019). وتختلف هذه المخاوف بين الأفراد في مختلف البلدان نتيجة للتباين في اللوائح والقوانين الوطنية (Bano, Mirza, Sohail & Javaid, 2022). بالإضافة إلى ذلك، يمتلك التشريع الحكومي ضماناً لحماية البيانات الشخصية من الاستخدام السيئ، كما يمتلك الأفراد الحق في مراجعة أو تصحيح هذه المعلومات إذا لزم الأمر (Al-Jabri, Eid & Abed, 2019).

(6-4-3-4-2) الرعاية الأخلاقية التنظيمية للخصوصية

اقتصر مفهوم الرعاية الأخلاقية التنظيمية Organizational Ethical Care فى الدراسات السابقة على علاقة الشركة بالعاملين فيها، إلا أن هذا المفهوم يمكن تطبيقه أيضاً في نطاق تعامل الشركة مع عملائها، تُعرف الرعاية الأخلاقية التنظيمية على أنها "قيم المنظمة التي تستند على تفضيل مصلحة العملاء" (Bano et al., 2022). فى حين تعرف الرعاية الأخلاقية التنظيمية للخصوصية على أنها "مستوى الاهتمام الحقيقي والدائم الذي توليه المنظمة للحد من المخاوف المتعلقة بخصوصية عملائها". يتضمن هذا المفهوم سلسلة من الاتجاهات والأنشطة التى تتعلق بالرعاية باعتبارها توجهاً أساسياً لتحقيق الخير للآخرين (Nicholson & Kurucz, 2019). تشمل الرعاية الأخلاقية العناية الحقيقية والدائمة تجاه مخاوف خصوصية العملاء. وتؤثر الممارسات الأخلاقية للمنظمة وسياسة الخصوصية على تعزيز الثقة، وتخفيض مخاوف الخصوصية، (Mattison Thompson & Siamagka, 2022; Singh, Sinha & Liébana -Cabanillas, 2020).

وعلى العكس من ذلك، فإن سوء التعامل مع معلومات العملاء الخاصة أو الكشف العرضي عنها، يزيد من حالات سرقة الهوية، والاختراق، والوصول غير المصرح به إلى حسابات العملاء. ويؤدي ذلك إلى مخاوف العملاء فيما تتعلق بالخصوصية عبر الإنترنت، وامتناعهم عن التعامل مع المواقع الإلكترونية (Bano et al., 2022).

إن الالتزام بالرعاية الأخلاقية التنظيمية يتجاوز حد الالتزام بالقواعد والقوانين المنصوص عليها في اللوائح التشريعية، وذلك باعتبارها جوهر كل تفكير وعمل تنظيمى، وتكمن قيمتها في العلاقة مع الآخرين ورعايتهم بطرق تؤدي إلى تعزيز رفاهيتهم (Gabriel, 2015).

وقد تتعارض أخلاقيات الرعاية التنظيمية مع التشريعات والقوانين الأخلاقية، التي تركز على الجانب العقلاني وتتجاهل الجانب العاطفي. حيث تُسلِّط أخلاقيات الرعاية التي تمارسها المنظمات الضوء على العلاقات العاطفية واحتياجات الناس، مما يعزز المزيد من الرعاية والرحمة تجاه جميع الأطراف المعنية. يُعطى هذا المفهوم الأولوية للأنشطة التي تنطوي على الرعاية باعتبارها توجهاً إنسانياً أساسياً تجاه الآخرين والمجتمع بأسره (Nicholson & Kurucz, 2019).

(6-4-4) العوامل المرتبطة بادارة التفاعل

تبرز شكوك ومقاومة العملاء تجاه استخدام روبوتات الدردشة الذكية في التفاعلات اليومية عبر الإنترنت، وتشمل بعض السلبيات مثل شعورهم بعدم الارتياح فى الحصول على الخدمة بواسطة الذكاء الاصطناعى (Pinochet, de Gois, Pardim & Onusic, 2024)، خاصة عند التفاعل مع الأمور الشخصية. إن إخبار العملاء بأن المحادثة ستتم بواسطة روبوتات الدردشة الذكية يؤدي إلى تقليل مدة التفاعل بشكل كبير، وإذا تم تنفيذ إدارة التفاعل بشكل فعال وشفاف مع مراعاة أدوات حماية البيانات فمن الممكن تقليل مخاوف المستخدمين بشأن الخصوصية عند التفاعل مع روبوتات الدردشة (Bartol et al., 2022). ويمكن توضيح العوامل المرتبطة بادارة التفاعل المؤثرة على مخاوف الخصوصية والتى تشملها الدراسة الحالية كما يلى:

(6-4-4-1) الحاجة إلى التفاعل البشري

تشير الدراسات فى علم النفس إلى أن الحاجة إلى التواصل مع الآخرين وتكوين علاقات شخصية معهم تعتبر من أهم الدوافع الأساسية التى تفسر قدر كبير من السلوك البشري (Baumeister & Leary, 2017). ويمكن تعريف الحاجة إلى التفاعل البشري من الجانب التسويقى على أنها "الرغبة في الاستمتاع بالاتصال الشخصي مع مقدمى الخدمة" (Dabholkar & Bagozzi, 2002).أما في سياق استخدام روبوتات الدردشة، فإنها تشير إلى ميل الأفراد إلى التواصل الشخصي مع مقدمى الخدمة بدلا من تلقي الخدمة عن طريق الروبوت (Rajaobelina et al., 2021).

لدى الشركات حافز قوي لاستبدال وكلاء خدمة العملاء البشريين بروبوتات الدردشة المدعمة بالذكاء الاصطناعي المثيرة للجدل بشأن أخلاقياتها، ومصداقيتها، وميلها لنشر معلومات خاطئة. في الوقت نفسه، يُظهر المستهلكون تقبلاً متبايناً تجاه خدمة العملاء القائمة على برامج الدردشة الآلية. من جهة أخرى تتفاوت حاجة العملاء للتفاعل البشري، وذلك لاختلافها من شخص لآخر بناءً على شخصياتهم، ويحتاج العملاء الاجتماعيين بشكل أكبر إلى التفاعل البشري مقارنة بغيرهم من العملاء الآخرين، وفى حالة عدم تحقيق ذلك، فقد يشعرون بالإحباط، وعدم الرضا (Lee, 2017). كما أنهم أكثر انتقاداً لبرنامج الدردشة الآلي عند استخدام روبوت الدردشة في الخدمة الإلكترونية، ويعتبرونه مرعب ومخيف (Ashfaq, Yun, Yu & Loureiro, 2020)، ويرجع السبب فى ذلك إلى رغبتهم القوية في التفاعل مع البشر. إذ يرون التفاعل البشري أكثر موثوقية ومتعة وسهولة من التفاعل الآلي (Xie, Chen & Guo, 2020). بالإضافة إلى ادراكهم لخلق القيمة العلائقية، سواء كان ذلك من خلال استمتاعهم بتطوير العلاقات مع مقدمى الخدمة وتحسين جودة التجربة، أو من خلال تجنب الأخطاء في تقديم الخدمة أو عدم الاستجابة (Immonen, Sintonen & Koivuniemi, 2018). إن الاستجابة الفورية من مقدمي الخدمة البشريين تعبر عن الكفاءة، إلا أن هذا الأمر لا ينطبق على روبوتات الدردشة، فالسرعة في تقديم الخدمة والاستجابات الفورية قد تبدو طائشة وغير طبيعية، كما أن التأخير فى الاستجابة يعبر عنه بالجدية فى العمل (Söderlund, Oikarinen & Tan, 2022).

(6-4-4-2) الأدوات التكنولوجية لدعم الخصوصية

تعتبر تكنولوجيا دعم الخصوصية Privacy Enhancing Technologies (PETs) مجموعة ناشئة من الأدوات التكنولوجية التي تساعد على استخراج نتائج مفيدة من البيانات. يمكن تعريف تكنولوجيا دعم الخصوصية، وفقاً لوكالة الاتحاد الأوروبي للأمن السيبراني على أنها "مجموعة من الأدوات التكنولوجية التي تساعد على عدم تزييف واختراق البيانات، وتوفير الخصوصية والأمان في حماية البيانات"(European Union Agency for Cybersecurity, 2023). يعتبر أمان البيانات وحمايتها جزءاً أساسياً في أي نظام لمعالجة البيانات، وتعد متطلباً قوياً في جميع أنظمة الحاسبات، لأن أي انتهاك للأمان يمكن أن يؤدي إلى وقوع كوارث في النظام بأكمله. وتساعد تكنولوجيا دعم الخصوصية في فهم العوامل التي تؤثر على قرارات حوكمة البيانات، وتقليل الأذى الناتج عن استخدامات البيانات الخاطئة (Rath & Kumar, 2021). كما تعمل على التحكم في الكشف عن البيانات، وتقليل التهديدات، وانتهاك الخصوصية (The Royal Society, 2023). ولا يقتصر خطر انتهاكات الخصوصية على المصادر الخارجية للشركات فحسب، بل قد يكون لها مصادر داخلية في بعض الأحيان (National Institute of Standards & Technology (NIST),2024).

تُولي الشركات اهتماماً بأمان البيانات بشكل عام، وتتحمل مسئولية حماية بيانات العملاء عند توفير تطبيقات روبوتات الدردشة، وخاصة فيما يتعلق بأنظمة المصادقة والدفع التي تضم معلومات حساسة. وفى المقابل، تقوم الشركات بجمع وتخزين واستخدام البيانات الشخصية للعملاء لأغراض تجارية وتسويقية (Adamopoulou & Moussiades, 2020). قد تثير تفاعلات العملاء والمستخدمين مع روبوتات الدردشة المخاوف من سوء الاستخدام وتسريب البيانات، خاصة إذا لم تطبق قواعد الخصوصية بشكل كافٍ، حيث يشارك العملاء معلوماتهم الشخصية مثل بطاقات الائتمان، وفى اعتقادهم أن بيئة الذكاء الاصطناعى آمنة (Sebastian, 2023). ولكن قد تُخزن نماذج الذكاء الاصطناعي هذه المعلومات مؤقتاً لمدة تصل إلى 30 يوم، مما يزيد من خطر اعتراض البيانات أثناء الإرسال إذا كانت القناة غير آمنة. وفى حالة حدوث أي من هذه المشاكل، فقد يؤثر ذلك بشكل كبير على ثقة المستخدم في أنظمة الذكاء الاصطناعي، مما يضر بسمعتها بشكل كبير(Choudhury & Shamszare, 2023).

(6-5) النتائج السلوكية المترتبة على مخاوف الخصوصية

تؤثر مخاوف الخصوصية بشكل كبير على سلوك المستخدمين، ويترتب عليها امتناعهم عن استخدام الخدمات عبر الإنترنت، وعدم الشراء، ورفض الإفصاح عن المعلومات الشخصية، أو تحريفها (Cottrill, Jacobs, Markovic & Edwards, 2020)، وتعتبر مخاوف الخصوصية قوة دافعة لمقاومة المستخدمين، مما يبرز أهمية حماية خصوصيتهم أثناء تفاعلهم عبر الإنترنت (Cheng et al., 2022; Liu, Yan & Hu, 2021). ويمكن توضيح النتائج السلوكية المترتبة على مخاوف الخصوصية فيما يلى:

(6-5-1) التجنب السلوكى

يتدرج سلوك العملاء فى استخدام التكنولوجيا من الاستخدام المفرط، إلى مجموعة متنوعة من السلوكيات السلبية مثل التجاهل، المقاومة، التجنب، وأخيراً الإنسحاب (Cao & Yu, 2019). وقد يظهر المستخدمون سلوك تجنب المعلومات قبل أن يقرروا الانسحاب من استخدام تكنولوجيا ما. ويتجاهل المستخدمون ويتجنبون بعض المعلومات بسبب نقص الوقت أو الطاقة أو المعرفة أو الاهتمام الشخصي (Guo, Lu, Kuang & Wang, 2020). ينشأ سلوك التجنب كاستجابة لتعرض الفرد للعديد من المثيرات، مثل التعامل مع الإعلانات المزعجة عبر الإنترنت، نتيجة لردود فعل عقلية مثل التجاهل، أو ردود فعل عاطفية مثل المشاعر السلبية. تتحول هذه المشاعر إلى سلوكيات للتجنب مثل توقف النشاط عبر الإنترنت، وتصفية الإعلانات، واستخدام برامج حجب الإعلانات،...وغيرها من السلوكيات السلبية (McKee, 2021).

قد ينشأ سلوك التجنب للتكنولوجيا بسبب مشاكل في تصميم الواجهة، أو نقص في الخدمات اللازمة لأداء المهام المطلوبة (Immonen et al., 2018). يظهر المستخدمون التجنب السلوكي قبل أن يقرروا الانسحاب أو الحظر لضمان عدم إتاحة الفرصة لاستهدافهم (Boerman, Kruikemeier & Bol, 2021).

يعتبر سلوك التجنب Avoiding behavior مفهوم متعدد الأبعاد، يتكون من التجنب الإدراكى والعاطفي والسلوكي. يُعرف التجنب الإدراكى على أنه استجابة للإدراك السلبي تدفع الفرد إلى تحويل انتباهه بعيداً عن شيء ما. أما التجنب العاطفي، فيتمثل في رد فعل عاطفي سلبي تجاه الشيء، مثل الكراهية الشديدة، الغضب، الإحباط ، الخوف. بينما ينشأ التجنب السلوكي نتيجة لمشاعر سلبية قوية (Youn & Kim, 2019). ويُعرَّف التجنب السلوكي بأنه "جميع الأفعال أو الإجراءات التى يستخدمها الأفراد لتفادي المواقف المحتملة الناتجة عن الضغط أو الضيق" (Dodoo & Wen, 2019). وتركز الدراسة الحالية على أفعال التجنب السلوكي، متجاوزة بذلك البعدين الإدراكى والعاطفي. ويعود السبب في ذلك إلى أن البعد الإدراكي، الذي يتضمن صرف الانتباه والنظر عمداً بعيداً عن موضع التهديد، ينتهي عادةً في شكل سلوكي، وقد يُصنف أحياناً كتجنب سلوكي (Stubenvoll et al., 2022). بالإضافة إلى ذلك، فإن البعد العاطفي للتجنب، يتشابه إلى حد كبير مع مخاوف الخصوصية في الدراسة الحالية. ونظراً لأن روبوتات الدردشة تشكل تهديداً لحق الأفراد في الخصوصية، فقد لا يكون تجاهلها كافياً.

(2-5-6) الإفصاح عن المعلومات

يعرف الإفصاح عن المعلومات Information Disclosure بأنه "الكشف الطوعي للأفكار والآراء، والمعتقدات، والمشاعر وغيرها من المعلومات الشخصية، التي يمكن أن تجعل الشخص عرضة للضعف أو الابتزاز" (Melumad & Meyer, 2020). كما يشير إلى "تبادل المعلومات الشخصية بين الأفراد كوسيلة للتواصل وبناء العلاقات. ويتضمن ذلك، الكشف عن الاهتمامات والهوايات والعلاقات، دون النظر إلى إمكانية استخدام هذه المعلومات في استهداف الأفراد" (Ni, 2023). وفى مجال التجارة الإلكترونية، يشير الإفصاح عن المعلومات عبر الانترنت إلى "سلوك العملاء فى مشاركة المعلومات الحساسة أو البيانات الشخصية مع مستخدمين آخرين أو البائعين عبر الانترنت "(Rodríguez-Priego et al., 2023). حيث يتمتع كل شخص بمساحة محددة من المعلومات التي يفضل كشفها أو إخفاؤها بشكل واضح، وتتأثر هذه الحدود بعوامل فردية مثل مستوى التحكم الذاتي، وبعوامل بيئية مثل القوانين التنظيمية والحكومية لحماية البيانات. ويختلف مدى حدود هذه المعلومات وفقاً لدرجة المرونة، والظروف الشخصية والبيئية لكل شخص (Al-Jabri et al., 2019).

وينشأ الإفصاح عن المعلومات نتيجة للمقارنة بين المزايا، والعيوب المحتملة للكشف عن المعلومات، وذلك وفقاً لنظرية حساب الخصوصية "Privacy Calculus Theory"، التى تقترح أن قرار الأفراد للكشف عن معلوماتهم الشخصية يعتمد على تقديرهم للمخاطر والفوائد المحتملة (Hong et al., 2021). وتعتمد هذه النظرية على مبادئ نظرية التبادل الاجتماعي، التي تركز على مقارنة الجوانب الإيجابية والسلبية التي يمكن أن تؤثر على قرار الأفراد بالكشف عن معلوماتهم الشخصية (Kroll & Stieglitz, 2021).

وللإفصاح عن المعلومات العديد من الجوانب الإيجابية مثل توفير الوقت والأموال، تعزيز الذات، التكيف الاجتماعي، المتعة والجدة، الإيثار، بناء العلاقات، الاستخدام المجاني للخدمات، تمكين المنظمة من التعرف على العملاء في المستقبل (Hong et al., 2021). من جهة أخرى، يتحمل الأفراد تكاليف وجوانب سلبية كثيرة نتيجة للإفصاح عن المعلومات تتضمن فقدان السيطرة، إساءة استخدام المعلومات، المخاطر الأمنية (Kroll&Stieglitz,2021). لذا يرتبط الإفصاح عن المعلومات ارتباطاً وثيقاً بالخصوصية. كما تؤثر الخصوصية بشكل كبير على قرار الأفراد بالكشف عن معلوماتهم الشخصية (Ni,

(2023. وبمقارنة المخاطر المتوقعة المرتبطة بالكشف عن المعلومات الشخصية، بقدرة الفرد على حماية نفسه من هذا التهديد، فإذا كانت المخاطر تفوق الفوائد، فمن المرجح أن يتجنب الشخص الكشف عن معلوماته الشخصية.

أما إذا شعر الفرد بأنه قادر على حماية نفسه من المخاطر المحتملة، فقد يكون أكثر استعداداً للكشف عن معلوماته الشخصية والمشاركة في المزيد من المعاملات الإلكترونية (Rodríguez-Priego et al., 2023).

يقرر العملاء الكشف عن معلوماتهم الشخصية عندما يشعرون بوجود عدالة إجرائية تحمي تلك المعلومات، مع تعويض مالي يشجعهم للإفصاح عنها. وتختلف درجة الإفصاح بناءً على شدة الحدث، واحتمالية حدوث التهديد، وفعالية التدابير الوقائية التى يتخذها العميل (Kruikemeier, Boerman & Bol, 2020). وقد يؤدي مشاركة المعلومات الشخصية لأطراف ثالثة دون موافقة العملاء إلى انتهاك "العقد الإجتماعي" الضمني بين العميل والشركة عبر الإنترنت. هذا العقد الإجتماعي الإفتراضي يجعل الأشخاص يشعرون بأن هناك اتفاقاً متبادلاً ضمنياً بأن كلاً منهما سوف يستخدم المعلومات الشخصية بشكل مسئول وعادل، عند مشاركتها مع الأطراف الأخرى (Boerman et al., 2021).

(7) الدراسات السابقة وتطوير فروض الدراسة

سيتم عرض الدراسات السابقة إعتماداً على العلاقة بين متغيرات الدراسة على النحو التالي:

(7-1) العلاقة بين العومل الفردية المرتبطة بمستخدمى روبوت الدردشة ومخاوف الخصوصية

أجرت دراسة Osatuyi (2015) تحليلاً لمعرفة تأثير الوضوح والقلق من استخدام الحاسب الآلى على مخاوف الخصوصية لمستخدمي وسائل التواصل الاجتماعي. كشفت النتائج عن وجود علاقة قوية بين درجة الوضوح ومستوى القلق من استخدام الحاسب الآلى، وكذلك بين هذين العاملين ومخاوف الخصوصية.

في سياق مماثل، أشارت دراسة Anic et al. (2019)، إلى استكشاف العلاقة بين العوامل الفردية والاجتماعية التي تؤثر على مخاوف الخصوصية والنية السلوكية لمستخدمي الإنترنت. ومقارنة الفوائد المدركة من قبل مستخدمي الإنترنت وشعورهم بمخاوف الخصوصية في البيئة الرقمية. وأظهرت النتائج أن القلق من استخدام الحاسب الآلى وإدراك جودة التشريعات الحكومية يعتبران من المسببات الهامة لمخاوف الخصوصية، فالأفراد الذين يعانون من مستويات عالية من قلق الحاسب الآلى يظهرون عدم الارتياح كما يشعرون بمستويات مرتفعة من مخاوف الخصوصية. كما تمثل الفوائد المدركة من استخدام الإنترنت العامل الرئيسي الذي يفسر النية في مشاركة المعلومات الشخصية وتبنى التكنولوجيا الجديدة.

وفي دراسة أخرى، سعت دراسة Inan et al. (2022)، إلى فهم كيفية تأثير القلق التكنولوجي والتأثير الاجتماعي على التبني التكنولوجي لخدمات نقل الركاب. وأظهرت النتائج أن مخاطر الخصوصية وتكلفة التعلم تؤثران على القلق التكنولوجي، وأن كلاهما يؤثر بشكل كبير على نية استخدام الخدمة. كما أن القلق التكنولوجي يؤثر على القيم السلبية مثل مخاطر الخصوصية وتكلفة التعلم، وكلاهما يؤثر سلبياً على اتجاه المستخدمين لتبنى تكنولوجيا خدمات النقل.

من جهة أخرى، في دراسة Zhang & Zhang (2024)، التى اهتمت بمعرفة تأثير مخاوف الخصوصية والضعف المدرك والقلق التكنولوجي على مقاومة الدفع عبر تطبيق التعرف على الوجوه (Facial Recognition Payment (FRP. أظهرت نتائج الدراسة ارتباطاً كبيراً بين الضعف المدرك لكل من التكنولوجيا المستخدمة، ومقدمي الخدمة، والجوانب القانونية، وبين زيادة مخاوف الخصوصية. فى حين أشارت الدراسة إلى أن القلق التكنولوجي لم يكن مؤثراً فى مخاوف الخصوصية.

كما سعت دراسة Ischen et al. (2020)، إلى معرفة تأثير روبوتات الدردشة ومواقع الويب ذات الخصائص الشبيهة بالبشر على مخاوف الخصوصية. وأظهرت النتائج أن روبوتات الدردشة ذات الخصائص البشرية تزيد من رغبة المستخدمين في

الكشف عن معلوماتهم الشخصية، وتقلل من مخاوفهم المرتبطة بالخصوصية مقارنة بروبوتات الدردشة ذات الخصائص الآلية.

كما أظهرت الدراسة أن المستخدمين يشعرون بمزيد من الراحة والألفة مع مواقع الويب مقارنة بروبوتات الدردشة، ولاحظت الدراسة اختلافاً ملحوظاً في مستوى الود والألفة وذلك لصالح روبوتات الدردشة ذات الخصائص البشرية.

فى المقابل، اهتمت دراسة Bouhia et al. (2022) بتحديد العوامل المؤثرة فى مخاوف الخصوصية المتعلقة بالتفاعلات مع روبوت الدردشة في قطاع التأمين. وأظهرت النتائج أن المخاوف المتعلقة بالخصوصية تتأثر في المقام الأول بالخوف، تليها المخاطر المدركة والحاجة إلى الخصوصية. وعلى العكس من ذلك ،أظهرت الدراسة أن التكيف مع روبوتات الدردشة لا يؤثر على مخاوف الخصوصية.

وبناءً على ما سبق يمكن صياغة الفروض التالية:

الفرض الأول ف1: يؤثر القلق التكنولوجى عند استخدام روبوت الدردشة تأثيراً إيجابياً على شعور العملاء بمخاوف الخصوصية.

الفرض الثانى ف2: تؤثر الألفة مع روبوت الدردشة تأثيراً سلبياً على شعور العملاء بمخاوف الخصوصية.

(2-7) العلاقة بين العومل المرتبطة بإدارة المعلومات ومخاوف الخصوصية

تشير الدراسات إلى أهمية القدرة على التحكم في المعلومات كعامل رئيسي يؤثر على مخاوف الخصوصية. فعندما يشعر المستخدمون بأنهم يتحكمون في معلوماتهم الشخصية، تتراجع مخاوفهم المتعلقة بالخصوصية ويزداد استعدادهم للكشف عنها (Mattison Thompson & Siamagka, 2022). يساهم التحكم في المعلومات بشعور الأفراد بالأمان ويشجعهم على البحث عن المعلومات الصحيحة ومشاركتها عبر الإنترنت (Tseng et al. 2022). ومن الدراسات التى اهتمت بتحديد العوامل التي تؤثر على مخاوف الخصوصية في استخدام وسائل التواصل الاجتماعي وتأثيرها على الإفصاح الذاتي، دراسة Alashoor et al. 2017) التى توصلت إلى أن الوعي بالبيانات الضخمة يزيد من مخاوف الخصوصية التى تؤثر سلبياً على نوايا المستخدمين في تقديم معلومات دقيقة. كما أظهرت النتائج أن الاتجاهات السلبية للخصوصية تزيد من مخاوف الكشف عن الذات، وأن التحكم المدرك في المعلومات يمكن أن يخفف من هذه المخاوف. بالإضافة إلى ذلك، تهدف دراسة Rodríguez-Priego et al. (2023) إلى معرفة محددات الإفصاح عن الذات أثناء التسوق من موقع أمازون، وعلاقتها بالرعاية المدركة للعملاء. وكشفت النتائج عن تأثير الرعاية المدركة للعملاء على كل من التحكم المدرك فى المعلومات والثقة، وظهر الأخير كوسيط رئيسي لتأثير كل من رعاية العملاء المدركة والمخاوف المتعلقة بالخصوصية على الإفصاح عن الذات. كما أوضحت النتائج أن التحكم المدرك فى المعلومات يرتبط ارتباطاً إيجابياً بالثقة وسلبياً بمخاوف الخصوصية.

من جانب آخر، تهدف دراسة Jozani et al. (2020) إلى استكشاف مسببات مخاوف الخصوصية وتأثيرها على مشاركة المستخدمين لتطبيقات الدفع الاجتماعي من أمازون، وتطبيقات وسائل التواصل الاجتماعى، بالاعتماد على نظرية التنمية متعددة الأبعاد. أظهرت النتائج أن المخاوف المتعلقة بالخصوصية تقلل من مستوى المشاركة، وتؤثر سلبياً على التحكم في الخصوصية وحساسية المعلومات. كما أشارت الدراسة إلى أن حساسية المعلومات لها تأثير إيجابى على مخاوف الخصوصية لكل من تطبيقات الدفع الاجتماعي، ووسائل التواصل الاجتماعى. كما أكدت العديد من الدراسات على تلك النتيجة باستخدام تطبيقات تتضمن تكنولوجيا ناشئة مثل المساعدين الافتراضيين والواقع المعزز (Ha,Chen,Capistrano, 2021; Harborth & Pape, 2021).

ومن الدراسات التجريبية دراسة Sun et al. (2023)، التى اهتمت بمعرفة مدى تأثير حساسية المعلومات ودور وكلاء المحادثة الافتراضية مثل Apple, Siri, Amazon, Alexa على مخاوف خصوصية المستخدمين. تم عرض 24 معلومة شخصية لطلاب الدراسات العليا لتقييم مدى حساسيتهم لهذه المعلومات. تم تقسيم المعلومات الشخصية إلى خمس فئات مختلفة وفقاً لمستوى حساسيتها.

وبناءً على هذا التصنيف، يُعد رقم جواز السفر والعنوان ورقم الهاتف من بين المعلومات الحساسة للغاية، بينما يُعتبر النوع وأنواع المعالم السياحية المفضلة والطعام المفضل من المعلومات غير الحساسة. وأظهرت النتائج أنه عندما يُطلب من الطلاب تقديم معلومات حساسة، يزداد شعورهم بمخاوف الخصوصية، والعكس صحيح. وتوصلت دراسة Tao et al. (2024)، إلى أن المعلومات الشخصية المتعلقة بالهوية الشخصية والمدفوعات الرقمية هي الأكثر حساسية في خدمات التجارة الإلكترونية، ويشعر العملاء بمخاطر عالية وانتهاك للخصوصية عندما تقوم المنظمات بجمع أو مشاركة معلوماتهم الحساسة مع أطراف أخرى، خاصة عند استخدام تطبيقات الهاتف المحمول، نظراً لتزايد مخاوف الخصوصية لدى المستخدمين نتيجة لحساسية المعلومات المطلوبة عند تنزيل التطبيق.

وبناءً على ما سبق يمكن صياغة الفروض التالية:

الفرض الثالث ف3: يؤثر إدراك العملاء للتحكم فى المعلومات تأثيراً سلبياً على شعورهم بمخاوف الخصوصية.

الفرض الرابع ف4: تؤثر حساسية العملاء للمعلومات تأثيراً إيجابياً على شعورهم بمخاوف الخصوصية.

(3-7) العلاقة بين العوامل المرتبطة بالبيئة ومخاوف الخصوصية.

يعتقد الأفراد أن القوانين التى تنظم جمع واستخدام معلوماتهم الشخصية وتحمي خصوصيتهم، تجعلهم أقل قلقاً بشأن التدخلات المحتملة في الخصوصية. وبالفعل وجدت الدراسات السابقة أن إدراك القوانين يؤثر على مدى إدراك الأفراد للخصوصية فى بيئة الإنترنت مثل دراسة Škrinjarić, Budak & Rajh (2019). كما أكدت دراسة Anic et al. (2019)، على أن إدراك جودة التشريعات الحكومية يعتبر من المؤثرات الهامة لمخاوف الخصوصية عبر الإنترنت، وأن التشريعات الحكومية الضعيفة وغير الفعّالة تزيد من مخاوف الخصوصية.

كما كشفت دراسة Khan (2024) عن أسباب مخاوف الخصوصية وتأثيرها على سلوك مشاركة البيانات بين مستخدمي LinkedIn، وذلك بجمع آرائهم واتجاهاتهم وردود أفعالهم حول استخدام المنصة. تشمل بيانات LinkedIn معلومات مكثفة مثل التاريخ المهني والتعليم وتفاصيل الاتصال، التى يمكن لأصحاب العمل استغلالها لمراقبة الموظفين، مما قد يؤثر سلبياً على حياتهم الخاصة. ويعتقد 33% من المشاركين أن التدخل الحكومي ضروري لحماية خصوصية البيانات، بينما يعتبر 33% آخرون أن LinkedIn ضرورة مهنية رغم ترددهم في مشاركة البيانات.

وأوضحت دراسة Bano et al. (2022)، أن التشريعات والقوانين الحكومية تؤثر إيجابياً على مخاوف الخصوصية، كما تؤثر على اقبال العملاء على التسوق الإلكترونى. فى حين أن الرعاية الأخلاقية التنظيمية وولاء العملاء يرتبطان سلبياً مع مخاوف الخصوصية. كما توسطت مخاوف الخصوصية في العلاقة بين التشريعات والقوانين الحكومية وإقبال العملاء على التسوق الإلكترونى، ولكنها لم تكن وسيطًا في العلاقة بين الرعاية الأخلاقية التنظيمية وإقبال العملاء على التسوق الإلكترونى.

إضافة إلى ذلك، أوضحت الدراسات فى مجال السلوك التنظيمى، أن الرعاية التنظيمية الأخلاقية تسهم في تخفيض القلق الناتج عن العمل وتزيد من المشاركة الإستباقية في الممارسات التنظيمية (Houghton, Pearce, Manz, Courtright & Stewart, 2015). أما بالنسبة لمجال سلوك المستهلك خاصة في عصر الذكاء الاصطناعي، أوضحت ثلاثة دراسات لكل

من(2022) Mattison Thompson & Siamagka، أن الرعاية الأخلاقية التنظيمية للخصوصية لها تأثير إيجابي على تخفيض مخاوف الخصوصية لدى المستهلكين وسلوكياتهم التخريبية الناتجة عنها. كما تعتبر عاملاً دافعاً إيجابياً لزيادة رغبتهم في المشاركة بالمعلومات والكشف عنها. وكذلك فى ظل أنظمة الذكاء الاصطناعي يمثل ضمان الخصوصية وحماية البيانات ضرورة أخلاقية (Khoury, Avila, Brunelle & Camara, 2023).

إن التزام المنظمات بالرعاية الأخلاقية لخصوصية العملاء، بتوفير الشفافية لاستخدام بياناتهم الشخصية وحمايتها، يمنحهم مزيداً من التحكم في بياناتهم ويزيد من ثقتهم وتفاعلهم الإيجابي للتسوق الإلكترونى (Carmeli, Brammer, Gomes & Tarba, 2017).

وتؤثر الممارسات الأخلاقية التنظيمية للخصوصية أيضاً على رضا العملاء، وتقلل من شعورهم بمخاوف الخصوصية. وعلى النقيض يؤدي التعامل السيئ مع معلومات العملاء الخاصة إلى زيادة مخاوف الخصوصية، وتخفيض رغبتهم فى التسوق الإلكترونى (Singh et al., 2020).

وبناءً على ما سبق يمكن صياغة الفروض التالية:

الفرض الخامس ف5: توافر القوانين والتشريعات الحكومية لحماية الخصوصية يؤثر تأثيراً سلبياً على شعور العملاء بمخاوف الخصوصية.

الفرض السادس ف6: تؤثر الرعاية الأخلاقية البنكية للخصوصية تأثيراً سلبياً على شعور العملاء بمخاوف الخصوصية.

(4-7) العلاقة بين العومل المرتبطة بإدارة التفاعل ومخاوف الخصوصية

يعد ضمان جودة البيانات أمراً حيوياً لمكافحة الهجمات العدائية التي تستغل نقاط الضعف في نماذج الذكاء الاصطناعي، والتي تتلاعب بسلوكها من خلال إدخال بيانات مزورة بعناية وهجمات كسر الحماية متعددة الخطوات التي تهدف إلى استخراج معلومات المستخدم الحساسة مثل أرقام بطاقات الائتمان. هذه الهجمات يمكن أن تؤدي إلى نتائج مضللة وخطيرة. وللتصدي لهذه الهجمات، يجب تأمين البيانات باستخدام أدوات أمنية قوية مثل التشفير والتحكم في الوصول، بالإضافة إلى تدريب نماذج الذكاء الاصطناعي بأمثلة عدائية لتعزيز مرونتها ضد الهجمات، مما يزيد من صعوبة اختراق البيانات، ويحسن من ضمان الخصوصية ويقلل المخاطر المرتبطة بهذه الهجمات (Hariri, 2023).

وقد أجرى كل من Følstad et al. (2018)، دراسة استكشافية لفحص العوامل المؤثرة على ثقة مستخدمي روبوتات الدردشة. وأظهرت الدراسة أن ثقة المستخدمين تعتمد على خصائص الروبوتات مثل جودة تفسيرها للطلبات، ودرجة التشبه بالبشر، وأسلوب عرضها، وشكلها. بالإضافة إلى عوامل ترتبط بالخدمة مثل الأمان والخصوصية المدركة. كما أظهرت الدراسة أن المستخدمين يولون اهتماماً خاصاً للخصوصية والأمان أثناء التفاعل مع روبوتات الدردشة، وذلك لزيادة وعي المستخدمين بالمخاطر المحتملة.

وفى دراسة حديثة اهتم Sebastian (2023)، بتحديد العوامل المتعلقة بحماية البيانات وتعزيز الخصوصية لروبوتات الدردشة، مع التركيز على ChatGPT، واستكشاف التحديات المزدوجة لحماية المعلومات الحساسة للمستخدم. وأظهرت الدراسة أن حوالي 75.6% من العينة أعربوا عن مخاوفهم الشديدة بشأن الخصوصية وحماية البيانات، وأن 92.5% من المشاركين على استعداد لاستخدام نظام الذكاء الاصطناعي من أجل تعزيز الخصوصية وحماية البيانات. كما اتفق تقريباً جميع المشاركين بنسبة 94.8% على أن أنظمة الذكاء الاصطناعي يجب أن تمتثل لقوانين حماية البيانات. ومن ثم فإن عدم توافر أدوات لحماية الخصوصية وأمن البيانات يؤدي إلى انخفاض الثقة في نظم الذكاء الاصطناعي، وزيادة مخاوف الخصوصية.

كما أوضحت دراسة Khan (2024) التى اهتمت بتوضيح أسباب مخاوف الخصوصية من استخدام منصة LinkedIn. أن نسبة صغيرة فقط من عينة الدراسة عبّرت عن ثقتها في إجراءات أمان المنصة، مما يبرز شكوكاً حول حماية البيانات. وأظهرت النتائج أن 20% من المستخدمين يقترحون توفير أدوات تساعد على إخفاء تفاصيل بعض المعلومات الشخصية. وأن 15% من المستخدمين يوصون باستخدام خوارزميات الذكاء الاصطناعي المتقدمة للكشف عن التتبع غير المصرح به ومنعه. كما تؤكد النتائج على ضرورة معالجة هذه المخاوف وتوفير أدوات الأمان للحفاظ على نزاهة المنصة، مع الدعوة إلى معايير تنظيمية لحماية بيانات المستخدمين.

وفى دراسة Ischen et al. (2020)، أجرى الباحثون تجربة لفهم تأثير روبوتات الدردشة ومواقع الويب التي تظهر خصائص تشبه البشر على مخاوف الخصوصية. وأظهرت النتائج أن روبوتات الدردشة التي تظهر خصائص تشبه البشر تزيد من رغبة المستخدمين في الكشف عن معلوماتهم الشخصية، وتخفض من مخاوفهم بشكل كبير مقارنة بالروبوتات ذات الخصائص الآلية.

كما أشارت دراسة Hu & Min (2023) إلى أن أجهزة الذكاء الاصطناعي لا تقتصر على كونها مجرد آلات، بل يمكن اعتبارها كيانات اجتماعية، ويمكن للأفراد أن يشعروا بالقلق بسبب احتمالية انتهاك خصوصيتهم، وهذا يعود جزئياً إلى دمج الكاميرات التي تشبه العين البشرية في هذه الأجهزة. وأظهرت الدراسة أن أجهزة الذكاء الاصطناعي التي تحاكي البشر تثير مخاوف أكبر بشأن الخصوصية مقارنة بالأجهزة الاصطناعية البسيطة والأجهزة اللوحية. وخلصت الدراسة إلى أن استخدام أجهزة الذكاء الاصطناعي ذات السمات البشرية ليس مفيدًا، إذ يثير المظهر البشري قلقاً وعدم ارتياح بشأن الخصوصية لدى العملاء.

إلا أن الدراسة التجريبية التي أجراها Rhim et al. (2024) أثبتت عكس ذلك. حيث ركزت الدراسة على مقارنة استخدام أسئلة الإستقصاء بالاعتماد على روبوت الدردشة الذي يشبه البشر (HASbot)، والنسخة الآلية (baselinebot)، على عينة من طلاب المرحلة الثانوية. تم إجراء تجربة الاستطلاع لمعرفة مدى إدراك المستجيبين للروبوتات، وتجربة التفاعل، وجودة البيانات. أظهرت الدراسة أن إدراك المستجيبين لروبوت الدردشة الذي يشبه البشر كان أكثر إيجابية مقارنةً بالنسخة الآلية. مع شعور الطلاب بمستويات أعلى من التشبه بالبشر والوجود الاجتماعي. كما قضى المستجيبون وقتاً أطول في التفاعل مع روبوت الدردشة الذي يشبه البشر، وأبدوا مستوى أعلى من الرضا. أما بالنسبة لجودة البيانات، فقد تفوق روبوت الدردشة الذي يشبه البشر. في حين لم يُلاحظ أدنى فرق في التفاوت في الاستجابة بين الروبوتين.

وبناءً على ما سبق يمكن صياغة الفروض التالية:

الفرض السابع ف7: تؤثر حاجة العملاء للتفاعل البشرى تأثيراً إيجابياً على شعورهم بمخاوف الخصوصية.

الفرض الثامن ف8: يؤثر توافر الأدوات التكنولوجية لدعم الخصوصية تأثيراً سلبياً على شعور العملاء بمخاوف الخصوصية.

(7-5) العلاقة بين شعور العملاء بمخاوف الخصوصية والتجنب السلوكي

أظهرت العديد من الدراسات في مجال التجارة الإلكترونية وجود تأثير سلبي لمخاوف الخصوصية على سلوكيات المستخدمين، وذلك لاستخدامهم استراتيجيات دفاعية مثل برامج حذف ملفات تعريف الارتباط، وتمويه الهوية بمعلومات وهمية عند إدراكهم لطلب الشركات معلومات زائدة عن الحاجة، وللتغلب على مخاوف الخصوصية. كما يميلون إلى حجب معلوماتهم أو الإنسحاب من العلاقة إذا أرادوا تجنب خطر إساءة استخدام المعلومات، مما قد يقيّدهم فى إتمام المعاملات (Maduku et al., 2023; Bandara, Fernando & Akter, 2021).

وفيما يتعلق بالإعلانات عبر الإنترنت، أظهرت دراسة Ham (2017) أن الأفراد الذين يشعرون بمخاوف شديدة بشأن الخصوصية يميلون إلى حماية أنفسهم بشكل أكبر بالتصدي لمثل هذه الممارسات ومقاومتها. كما بينت الدراسة ارتباط مخاوف الخصوصية إيجابياً بسلوك التجنب. وفى نتائج مماثلة تم تأكيدها أيضاً في دراسة Aiolfi, Bellini & Pellegrini (2021)، وجد الباحثون أن نية التجنب مرتبطة بشكل إيجابي بمخاوف الخصوصية. وفي دراسة أجراها Jayasuriya, Udadeniya & Yalegama (2021)، بهدف معرفة أسباب رفض العملاء في سريلانكا للإعلانات عبر الإنترنت وتحديد العوامل الرئيسية التي تؤثر في هذا السلوك، توصلت النتائج إلى أن القلق بشأن الخصوصية، والشكوك حول الإعلانات، والتجارب السلبية تزيد من احتمالية سلوك الرفض.

أما في دراسة Singaraju et al. (2022)، فقد أوضحت كيفية تأثير العوامل الإدراكية على نية تجنب الإعلانات المخصصة على منصة YouTube. وكشفت النتائج عن وجود علاقة إيجابية بين مخاوف الخصوصية والنية في تجنب الإعلانات، بالإضافة إلى وجود علاقة سلبية بين عنصر الترفيه والنية في تجنب الإعلانات.

وبالتطبيق على وسائل التواصل الاجتماعى تناولت دراسة Wang, Ahmed & Bee (2024) تأثير استخدام الأخبار التعبيرية، والمناقشات السياسية، والمشاعر السلبية للمستخدمين مثل القلق والخوف من المراقبة، على التجنب الانتقائي لوسائل التواصل الاجتماعي. وأظهرت النتائج أن الأشخاص الذين يستخدمون الأخبار التعبيرية بكثرة ويشاركون في مناقشات سياسية ويشعرون بالقلق والخوف من المراقبة، هم الأكثر اعتياداً على التجنب الإنتقائي.

وبالتطبيق على إنترنت الأشياء (IoT)، أظهرت دراسة Lee, Ha, Oh & Park (2018)، التأثير السلبى لمخاطر الخصوصية المدركة على رغبة المستخدمين في التفاعل مع تلك التكنولوجيا. وبالمثل، الدراسة التى أجراها Vimalkumar, Sharma, Singh & Dwivedi (2021)، التي استهدفت معرفة إدراك المستهلكين لمخاوف الخصوصية وتأثيرها على قبول مساعدي الذكاء الاصطناعي الحواري. وجدت الدراسة أن المخاوف المتعلقة بالخصوصية لها تأثير سلبي على رغبة المستخدمين ونواياهم في التفاعل مع التكنولوجيا.

وبناءً على ما سبق يمكن صياغة الفرض التالي:

الفرض التاسع ف9 : يؤثر شعور العملاء بمخاوف الخصوصية من استخدام روبوت الدردشة تأثيراً إيجابياً على التجنب السلوكى.

(6-7) العلاقة بين شعور العملاء بمخاوف الخصوصية والإفصاح عن المعلومات

أظهرت الدراسات السابقة أن مخاوف الخصوصية تعتبر عاملاً أساسياً للإفصاح عن الذات، وترتبط سلبياً مع استعداد الأفراد للكشف عن بياناتهم الشخصية. بمعنى آخر، كلما زادت مخاوف الأفراد بشأن خصوصيتهم، كلما انخفض استعدادهم للمشاركة أو الإفصاح عن معلوماتهم الشخصية لجهة خارجية (Ischen et al., 2020).

وفي دراسة تجريبية أجراها Olt & Wagner (2020)، لتقييم العلاقة بين أمان نظام المعلومات وخصوصية المعلومات كهدفين متضاربين لمقدمى الخدمة، وجدت الدراسة أن مخاوف الخصوصية تعوق نية الأفراد في استخدام خدمات الحماية. كما قدمت الدراسة دليلاً على أن المستخدمين الحاليين وغير الحاليين للنسخ الاحتياطي عبر الإنترنت لا يختلفون في ادراكهم لتهديدات الأمان، ولكن يختلفون في مخاوفهم المدركة بشأن الخصوصية. وهذا يشير إلى أن مخاوف الخصوصية تُعتبر عائقاً رئيسياً للاستخدام، حتى إذا كان المستخدمون يشعرون بالأمان.

وفى دراسة أجراها Le, Zhang & Liu (2024) هدفت إلى معرفة أسباب سلوك الإفصاح عن الخصوصية في تطبيقات الهواتف المحمولة من خلال منظور الدعم الاجتماعي عبر الإنترنت. وأظهرت النتائج أن الدعم الإلكتروني للمعلومات

والعواطف يمتلك تأثيرات إيجابية على سلوك الإفصاح عن الخصوصية، بينما كان لمخاوف الخصوصية تأثير سلبي كمتغير وسيط. كما كشفت النتائج عن اختلاف في النتائج بناءً على النوع، حيث كان للإناث مستويات أعلى من مخاوف الخصوصية ومستويات أقل من الإفصاح عن الخصوصية.

وقد أجرت دراسة Ischen et al. (2020) تحليلاً لتأثير روبوتات الدردشة على مخاوف الخصوصية والإفصاح عن المعلومات. وأظهرت النتائج أن استخدام روبوت الدردشة الشبيه بالإنسان يساعد على انخفاض شعور المستخدمين بمخاوف الخصوصية مقارنة بروبوت الدردشة الآلى، كما يساعد على زيادة الرغبة فى الإفصاح عن المعلومات. وفى تجربة أجراها Roozen et al. (2022) لتحليل تأثير ربوتات الدردشة الآلية على مشاعر ونوايا المستهلكين لاستخدامها، ومعرفة تأثير مخاوف الخصوصية على الإفصاح عن المعلومات بالتطبيق على مجال مستحضرات التجميل، عبر منصتين مختلفتين عبر الإنترنت، وهما فيسبوك وموقع الشركة. أظهرت النتائج أن التفاعل مع الدردشة الآلية على الفيسبوك أدى إلى تحسينات أقل في المشاعر الإيجابية ونوايا الاستخدام، مقارنة بتفاعل المستخدمين على موقع الشركة.

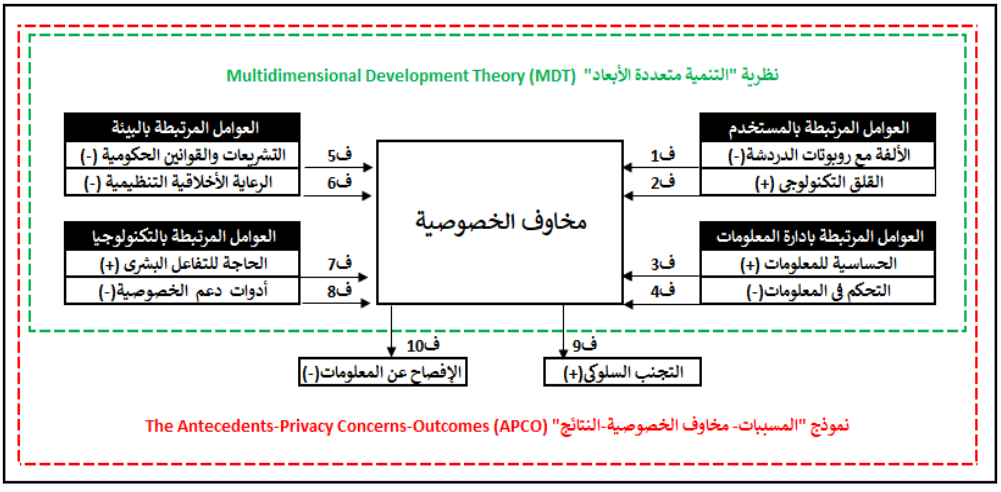
وكان لهذه العلاقة تأثير في زيادة مخاوف الخصوصية ورفض الإفصاح عن المعلومات. كما أظهرت النتائج تأثيراً أقوى لمخاوف الخصوصية عند التفاعل مع الدردشة الآلية على الفيسبوك مقارنة بالتفاعل على موقع الشركة. وأيضاً كان لهذه المخاوف تأثيراً كبيراً على رفض الإفصاح عن المعلومات.

وبناءً على ما سبق يمكن صياغة الفرض التالي:

الفرض العاشر ف10: يؤثر شعور العملاء بمخاوف الخصوصية من استخدام روبوت الدردشة تأثيراً سلبياً على الإفصاح عن المعلومات.

(8) نموذج الدراسة

في ضوء الدراسات السابقة والدراسة الإستكشافية، وبناءً على الدمج بين نظرية "التنمية متعددة الأبعاد" (MDT)، ونموذج "المسببات - مخاوف الخصوصية – النتائج" (APCO)، يمكن تمثيل متغيرات الدراسة والعلاقات بينها فى نموذج الدراسة فى الشكل (2).



شكل 2: نموذج الدراسة

المصدر: من إعداد الباحثة في ضوء الدراسات السابقة

(9) منهجية الدراسة

تعتمد الدراسة الحالية على المنهج المختلط Mixed Method للحصول على فهم أعمق وتحليلات شاملة لمخاوف العملاء بشأن الخصوصية عند استخدام روبوتات الدردشة، والتى لا تزال غامضة خاصة فى الأسواق الناشئة ذات الموارد المحدودة. تم استخدام هذا المنهج من قبل العديد من الباحثين في دراسات سابقة مثل دراسة (Liu, Hu, Yan & Lin 2023; Griffin et al. 2021; Sidaoui, Jaakkola & Burton,2020).

للتحقق بشكل أفضل من موثوقية واتساق النتائج، بدأت الدراسة بالمرحلة النوعية، وذلك بإجراء دراسة استكشافية (Creswell & Plano Clark, 2017). تم استخدام المقابلات المتعمقة لجمع معلومات شاملة، وتوضيح العديد من النقاط من خلال التفاعل مع المشاركين (Malhotra, 2020)، بهدف تحديد العوامل المؤثرة على مخاوف العملاء بشأن الخصوصية عند استخدام روبوت الدردشة في الخدمة البنكية، والنتائج السلوكية المترتبة على هذه المخاوف. تم الكشف عن عوامل جديدة قد تكون غير متوقعة وتطوير إطار مفاهيمي اعتماداً على إجراء المقابلات في هذه المرحلة، إضافة إلى الإستناد إلى ما جاء فى الدراسات السابقة. بناءً على نتائج الدراسة الاستكشافية، تم الانتقال إلى المرحلة الكمية وذلك بإجراء دراسة استنتاجية لتقييم صحة وثبات مقاييس الدراسة، وإختبار العلاقات بين المتغيرات (Malhotra, 2020) وفقاً للنموذج المقترح كما هو موضح في الشكل (2).

(9-1) مجتمع وعينة الدراسة

يشمل مجتمع الدراسة جميع عملاء البنوك العاملة فى مصر الذين يستخدمون خدمة روبوت الدردشة عبر المواقع الإلكترونية للبنوك في محافظتي القاهرة والجيزة. تم اختيار هاتين المحافظتين لأنهما تحتويان على النسبة الأكبر من فروع البنوك مقارنة بباقي المحافظات، كما هو موضح في الملحق (1).

تم اختيار البنوك المدرجة في الدراسة باستخدام طريقة الحصر الشامل للبنوك العاملة في مصر، والتي توفر خدمة روبوتات الدردشة عبر مواقعها الإلكترونية حتى تاريخ 29 فبراير 2024، وقد بلغت (6) بنوك، تم تحديدها بناءً على مراجعة مواقعها الإلكترونية، وهى : بنك مصر، البنك التجاري الدولي، بنك القاهرة، بنك كريدي أجريكول، بنك تنمية الصادرات، وبنك أبو ظبي التجاري.

تم اختيار عينة الدراسة من العملاء المستفيدين من تلك الخدمة، والذين استخدموا روبوت الدردشة مرة واحدة على الأقل، وذلك بالاعتماد على العينة الاحتمالية المنتظمة، نظراً لوجود إطار للعينة ولكن لصعوبة الحصول عليه تم تشكيل عينة منتظمة من عملاء البنك باستخدام أرقام جهاز الإستدعاء الآلى بالفرع، باتباع الخطوات التالية:

- تحديد عدد العملاء الذين يزورون البنك خلال فترة معينة (إسبوع).
- تحديد حجم العينة باستخدام الأساليب الإحصائية الحديثة مثل برنامج "STATS™ 2.0" كما هو موضح في الملحق (2)، وذلك باعتبار حجم عملاء البنوك أكثر من 500000 عميل، بدرجة ثقة 95%، وتم حساب العينة لتصل إلى 384 مفردة.
- حساب مدى العينة: وذلك بقسمة عدد العملاء (خطوة 1) على حجم العينة المرغوبة (خطوة 2).
- اختيار نقطة البداية بشكل عشوائي من أرقام جهاز الإستدعاء الآلى بالفرع من 1- 10.
- اختيار العينة، وذلك بالبدء بالعميل الذي تم اختياره عشوائياً كنقطة بداية، ثم اختيار كل عميل بعد إضافة مدى العينة للوصول لحجم العينة المطلوب. تضمن هذه الطريقة فرصة متساوية للاختيار لكل عميل، مما يوفر

عينة ممثلة لعملاء البنك. تم تدريب مجموعة من جامعى البيانات المحترفين لتجميع البيانات، بعد مراعاة جميع الظروف التي قد يتواجد فيها العملاء، مثل بداية الأسبوع ومنتصفه ونهايته، بالإضافة إلى مختلف أوقات اليوم من الساعه 8:30 صباحاً حتى الساعه الثالثة عصراً، كما تم توزيع الخدمة على مدار الأسابيع والشهور بشكل متنوع ومتوازن، ويتضح من الجدول (2) توزيع عينة الدراسة على البنوك التى تقدم خدمة روبوتات الدردشة حتى 29 فبراير 2024.

جدول 2: توزيع عينة الدراسة طبقاً لعدد فروع البنوك التى تقدم خدمة روبوت الدردشة فى محافظتى القاهرة والجيزة*

اسم روبوت الدردشة	البنوك		محافظة القاهرة	محافظة الجيزة	الإجمالى	النسبة	عينة البنوك
عبقرينو Abqarino	**بنك مصر**	**عدد الفروع**	**194**	**73**	**267**		
		النسبة	%73	%27	%100	%47	180
		عينة العملاء طبقاً لعدد الفروع	131	49	180		
زكى Zaki	**البنك التجارى الدولى**	**عدد الفروع**	**89**	**31**	**120**		
		النسبة	%74	%26	%100	%22	84
		عينة العملاء طبقاً لعدد الفروع	60	21	81		
Chat BDC	**بنك القاهرة**	**عدد الفروع**	**65**	**21**	**86**		
		النسبة	%76	%24	%100	%15	58
		عينة العملاء طبقاً لعدد الفروع	44	14	58		
Banki chat	**كريدى اجريكول**	**عدد الفروع**	**32**	**15**	**47**		
		النسبة	%68	%32	%100	%8	32
		عينة العملاء طبقاً لعدد الفروع	22	10	32		
ELINA	**بنك تنمية الصادرات**	**عدد الفروع**	**16**	**8**	**24**		
		النسبة	%67	%33	%100	%4	16
		عينة العملاء طبقاً لعدد الفروع	**11**	**5**	32		
AREF	**بنك ابوظبى التجارى**	**عدد الفروع**	**18**	**5**	**23**		
		النسبة	%78	%22	%100	%4	16
		عينة العملاء طبقاً لعدد الفروع	12	4	16		
		المجموع			**567**	%100	**384**

المصدر: من اعداد الباحثة من واقع بيانات البنك المركزى المصرى، الإدارة العامة للرقابة على البنوك، ادارة الشئون المصرفية، 2023، ملحق (1)

*لم تشتمل الدراسة على بنك المصرف المتحد على الرغم من تقديمه للخدمه يوم 15-2-2024، إلا أنها لم تكن مفعلة حتى 29-2-2024.

(2-9) أداة ومقاييس الدراسة

اعتمدت الدراسة فى جمع البيانات على قائمة الإستقصاء، وتمت مراجعة مسودة الإستقصاء الأولية من قبل أساتذة ذوي خلفية بحثية واسعة النطاق في مجال التسويق، وتكنولوجيا المعلومات، للتأكد من الصدق الظاهرى (Malhotra, 2010). وبناءً على تعليقاتهم، تم إجراء تعديلات طفيفة على الإستقصاء، والذي تم تجربته لاحقاً باختبار أولى Pre-Test على (31) عميل للتحقق من ثبات المقاييس المستخدمة، ومراجعة قائمة الإستقصاء من حيث وضوح العبارات، ومتوسط الوقت الذي يحتاجه العملاء لملئ القائمة، وصعوبة بعض الكلمات كما يراها المشاركون. وأسفرت الدراسة عن إعادة صياغة بعض العبارات التي تعتبر صعبة الفهم. كما تمتعت جميع المقاييس بثبات داخلي عالي كما هو موضح بالجدول (3)، حيث تراوحت معاملات ألفا كرونباخ بين (0.733، 0.845) وهو أعلى من 0.7 (Hair et al., 2019). وتتكون القائمة من ثلاثة أقسام يمكن توضيحها كما يلى:

القسم الأول: أسئلة التصفية، لاستبعاد المشاركين الذين لا تنطبق عليهم شروط الدراسة، مثل هل أنت عميل لهذا البنك؟. هل سبق لك استخدام روبوتات الدردشة للحصول على الخدمة البنكية ؟. مع عرض صور لشكل روبوتات الدردشة من مواقع البنوك لاختيار روبوت الدردشة المناسب الذى يتفاعل معه للتأكد من دقة الإجابات التالية ملحق (3).

القسم الثانى : يقيس متغيرات الدراسة والتى تحتوى على (43) عبارة والتى تعكس العوامل المؤثرة على مخاوف الخصوصية (المتغيرات المستقلة)، ومخاوف الخصوصية (المتغير الوسيط)، والنتائج السلوكية المترتبة علي مخاوف الخصوصية (المتغيرت التابعة). وفقاً لمقياس ليكرت الخماسى، الذى يتراوح بين (5) التى تشير إلى "موافق تماماً"، (1) وتشير إلى "لا أوافق على الإطلاق"، ويوضح الجدول (4) المقاييس التى اعتمدت عليها الباحثة فى قياس متغيرات الدراسة.

القسم الثالث: يتعلق بالخصائص الديموجرافية للعملاء، من حيث النوع، الفئة العمرية، مستوى الدخل، المؤهل الدراسى، عدد سنوات التعامل مع البنك باستخدام الموقع الإلكترونى، مستوى المتابعة لروبوتات الدردشة فى الخدمة البنكية.

جدول 3: اختبار الثبات لمقاييس الدراسة وفقا للإختبار الأولى Pre-Test

المتغيرات	البنود	الارتباط بين البنود الصحيحة	قيمة ألفا كرونباخ إذا تم حذف البند	قيمة ألفا كرونباخ	المتغيرات	البنود	الارتباط بين البنود الصحيحة	قيمة ألفا كرونباخ إذا تم حذف البند	قيمة ألفا كرونباخ
القوانين الحكومية	Q1	.662	.833	.845	الحساسية من المعلومات	Q23	.742	.644	.800
	Q2	.758	.752			Q24	.562	.728	
	Q3	.732	.769			Q25	.655	.715	
الرعاية الأخلاقية التنظيمية للخصوصية	Q4	.454	.752	.773	الحاجة إلى التفاعل البشرى	Q26	.643	.816	.833
	Q5	.561	.732			Q27	.801	.663	
	Q6	.714	.702			Q28	.647	.819	
	Q7	.609	.723		الأدوات التكنولوجية لدعم الخصوصية	Q29	.519	.791	.799
	Q8	.693	.713			Q30	.672	.717	
	Q9	.695	.708			Q31	.732	.685	
	Q10	.034	.610			Q32	.536	.785	
	Q11	.080	.710		مخاوف الخصوصية	Q33	.396	.717	.733
القلق التكنولوجى	Q12	.380	.500	.737		Q34	.668	.668	
	Q13	.747	.585			Q35	.426	.706	

المتغيرات	البنود	الارتباط بين البنود الصحيحة	قيمة ألفا كرونباخ إذا تم حذف البند	قيمة ألفا كرونباخ	المتغيرات	البنود	الارتباط بين البنود الصحيحة	قيمة ألفا كرونباخ إذا تم حذف البند	قيمة ألفا كرونباخ
الألفة مع روبوتات الدردشة	Q14	.441	.725	.836		Q36	.553	.682	
	Q15	.674	.601			Q16	.511	.685	
	Q16	.776	.740			Q17	.350	.730	
	Q17	.674	.789			Q18	.353	.723	
	Q18	.678	.791		الإفصاح عن المعلومات	Q37	.693	.867	.873
التحكم فى المعلومات	Q19	.663	.742	.804		Q38	.812	.767	
	Q20	.639	.753			Q39	.777	.804	
	Q21	.654	.745		التجنب السلوكى	Q40	.537	.646	.704
	Q22	.601	.763			Q41	.562	.634	
						Q42	.560	.632	
						Q43	.463	.658	

المصدر: من اعداد الباحثة من واقع استخدام برنامج SPSS 28.

تم تصميم قائمة الإستقصاء باستخدام Google Form، ثم تحويله إلى رمز مرئى QR Code لتسهيل وصول العملاء إليه باستخدام هواتفهم المحمولة، تم تقديم تعريف موجز لروبوتات الدردشة الموجودة على مواقع البنوك لجميع المشاركين ملحق (4). كما تم اتباع اسلوب متحفظ لاستبعاد القوائم التي استغرقت أقل من 9 دقائق لإستكمالها. وكان من المتوقع أن تستغرق بناء على الاختبار الأولى ما يقرب من 14 دقيقة. وكان متوسط مدة الاستقصاء للإجابات النهائية هو 18 دقيقة. تم اختيار نقطة فاصلة تستغرق 9 دقائق تشير إلى أن المشاركين الذين تم استبعادهم قضوا أقل من نصف وقت المشارك العادي للإستقصاء. تم تضمين أسئلة إسقاط فى الإستقصاء (مثل: إذا قرأت هذا السؤال، يرجى الإجابة على رقم 4)، تم حذف المشاركين الذين يظهرون أنماطاً متكررة في إجاباتهم من العينة النهائية. تم جمع (410) قائمة، واستبعاد (45) قائمة باتباع الإجراءات السابقة، مما أسفرعن (365) قائمة صحيحة، بمعدل استجابة قدره 0.89%.

جدول 4: مقاييس متغيرات الدراسة

متغيرات الدراسة	عدد العبارات	أرقام العبارات	المقاييس
التشريعات والقوانين الحكومية	3	(3-1)	(Lwin et al., 2007)
الرعاية الأخلاقية التنظيمية للخصوصية	8	(11-4)	(Mattison Thompson & Siamagka, 2022)
القلق التكنولوجى	4	(15-12)	(Venkatesh & Bala, 2008)
الألفة مع روبوتات الدردشة	3	(18-16)	(Bouhia et al.,2022)
التحكم فى المعلومات	4	(22-19)	(Xu, 2007)
الحساسية من المعلومات	3	(25-23)	(Dinev, Xu, Smith & Hart, 2013)
الحاجة إلى التفاعل البشرى	3	(28-26)	(Rajaobelina et al., 2021)
الأدوات التكنولوجية لدعم الخصوصية	4	(32-29)	(Hong, Chan & Thong, 2021)
مخاوف الخصوصية	4	(36-33)	(Bouhia et al., 2022)
الإفصاح عن المعلومات	3	(39-37)	(Gabisch & Milne, 2013; Malhotra et al., 2004)
التجنب السلوكى	4	(43-40)	(Jain & Purohit, 2022; Cho, & Cheon, 2004)

المصدر: من اعداد الباحثة من واقع الدراسات السابقة.

(3-9) توصيف عينة الدراسة.

تتألف عينة الدراسة كما فى جدول (5) بشكل رئيسي من عملاء البنوك الذين تتراوح أعمارهم بين 30 - 50 عاماً بنسبة 76%. وكان أكثر من نصف المستجيبين من الذكور بواقع 61%، والحاصلين على مؤهل جامعى بنسبة 69%. كما أفاد 48% من المشاركين بالتعامل مع مواقع البنك الإلكترونية لأكثر من 3 سنوات، كما كان مستوى المتابعة لروبوتات الدردشة فى الخدمة البنكية منخفض بنسبة 72%.

جدول 5: توصيف عينة الدراسة

الخصائص	النوع			المؤهل الدراسى			
	ذكر	أنثى	الإجمالى	طالب جامعي	مؤهل جامعي	دراسات عليا	الإجمالى
التكرار	223	142	365	18	251	96	365
النسبة	%61	%39	%100	%5	%69	%26	%100
الخصائص	مستوى الدخل				الفئة العمرية		
	أقل من 15000	15000-40000	أكثر من 40000	الإجمالى	30-18	50-30	أكثر من 50	الإجمالى
التكرار	25	305	35	365	59	279	27	365
النسبة	%7	%83	%10	%100	%16	%76	%8	%100
الخصائص	عدد سنوات التعامل مع البنك باستخدام الموقع الإلكترونى				مستوى المتابعة لروبوتات الدردشة فى الخدمة البنكية			
	أقل من سنه	2-3	أكثر من 3 سنوات	الإجمالى	منخفض	متوسط	مرتفع	الإجمالى
التكرار	40	149	176	365	264	62	39	365
النسبة	%11	%41	%48	%100	%72	%17	%11	%100

المصدر: من اعداد الباحثة من واقع الدراسة الميدانية.

(4-9) التحليل الوصفى لمتغيرات الدراسة

يوضح الجدول (6) التحليل الوصفى لمتغيرات الدراسة من حيث الوسط الحسابى والإنحراف المعيارى باستخدام برنامج التحليل الإحصائى (SPSS ver.28). وبالنظر لنتائج الوسط الحسابى الواردة فى الجدول يتضح أن أكثر المتغيرات قبولاً هو التحكم فى المعلومات، بينما الأدنى قبولاً هو الحاجة للتفاعل البشرى.

جدول6: التحليل الوصفى لمتغيرات الدراسة

المتغيرات	الوسط الحسابى	الانحراف المعيارى
القوانين والتشريعات الحكومية	3.5091	.86995
القلق التكنولوجى	3.1148	.80375
الألفة مع روبوتات الدردشة	2.9918	.92641
الحاجة للتفاعل البشرى	2.5607	.95712
التحكم فى المعلومات	3.9803	.72878
الحساسية للمعلومات	3.2654	.88581
الأدوات التكنولوجية لدعم الخصوصية	3.0788	.92505

المتغيرات	الوسط الحسابى	الانحراف المعيارى
مخاوف الخصوصية	3.0550	.86928
الإفصاح عن المعلومات	2.7582	.86813
التجنب السلوكى	2.9939	.90570
الرعاية الأخلاقية التنظيمية للخصوصية	3.5068	.88101

المصدر: من اعداد الباحثة من واقع التحليل الإحصائى

كما يتضح أن معظم متغيرات البحث يتجاوز فيها الوسط الحسابى عن (3)، مما يدل على أن لها درجة قبول جيدة لدى عينة الدراسة، كما أن بقية المتغيرات يتجاوز الوسط الحسابى فيها عن (2.5) مما يدل على ميل رأى عينة الدراسة إلى الحيادية. كما تقاربت أيضاً قيم الإنحراف المعيارى لمتغيرات الدراسة، والتي تراوحت بين (0.95712، 0.72878) مما يدل على تقارب آراء العينة حول متغيرات الدراسة.

(5-9) التحليل الإستنتاجى

اعتمدت الدراسة الحالية على طريقة المربعات الصغرى الجزئية لنمذجة المعادلة الهيكلية Partial Least Squares Structural Equation Modeling (PLS-SEM)، الذى يوفر مرونة أكبر بكثير من نمذجة المعادلة الهيكلية القائمة على التباين المشترك (CB-SEM)، كما لا يفترض ضرورة التوزيع الطبيعى للبيانات (Hair, Hult, Ringle, Sarstedt, Danks & Ray, 2021)، والسماح باختبار نماذج أكثر تعقيداً، والتي تعتمد على وجود متغيرات وسيطة أو تأثيرية (Hair et al., 2020, 2016). تم تطبيق طريقة المربعات الصغرى الجزئية لنمذجة المعادلة الهيكلية على مرحلتين 1) تقييم نموذج القياس ، 2) تقييم النموذج الهيكلى (Hair et al., 2019).

(1-5-9) تقييم نموذج القياس

يهدف تقييم نموذج القياس للتأكد من صدق وثبات مقاييس الدراسة، وذلك كما يلى:

- اختبار الثبات: تمت دراسة مدى الاتساق الداخلي لمتغيرات الدراسة باستخدام معامل كرونباخ ألفا ومعامل الثبات المركب، حيث تم حساب القيم وفقاً للجدول (7). وأظهرت نتائج التحليل أن متغيرات الدراسة تتمتع بدرجة عالية من الاتساق الداخلي. وأن جميع قيم معاملات كرونباخ ألفا والثبات المركب تجاوزت القيمة المعيارية 0.7، فيما عدا المتغيران الإفصاح عن المعلومات، الرعاية الأخلاقية التنظيمية للخصوصية حيث تقع قيمة الفا كرونباخ أدنى من القيمة المعيارية بشكل طفيف 0.699، 0.7 على التوالى، وقد حاولت الباحثة تحسين قيمة معامل كرونباخ لكل منهما بحذف بعض العناصر المكونة للمتغير. ومع ذلك، لم يظهر أي تحسن في القيمة بعد حذف أي عنصر من العناصر مما يدل على أن لكل عنصر دور فريد في تحديد قوة الاتساق الداخلي.

وبما أن حذف أي عنصر لم يسفر عن التحسين، فإن الباحثة اتخذت قراراً بالاحتفاظ بالنتيجة كما هي، رغم عدم تحقيق التحسين المطلوب، مع إمكانية حذف هذه العناصر لاحقاً إذا لزم الأمر.

كما أن نتيجة لوجود بعض العيوب لمعامل مقياس ألفا كرونباخ منها حساسيته الشديدة لعدد العناصر المكونة للمتغير التي تقل عن 10، ويمكن أن يعطي نتائج مختلفة بتغيير عدد البنود، وقد يكون من المفيد استخدام أدوات أخرى إضافية لضمان الدقة والشمول في اختبار الثبات مثل معامل الثبات المركب والإكتفاء به في حالة تحليل نمذجة المعادلة الهيكلية وذلك لتلافي عيوب معامل كرونباخ (Hair et al., 2010; Malhotra et al., 2010).

جدول 7: نتائج الثبات

متغيرات الدراسة / الإختبار الإحصائى	الإتساق الداخلي Cronbach's Alpha	الثبات المركب Composite Reliability
التشريعات الحكومية	0.749	0.856
القلق التكنولوجى	0.722	0.825
الألفة مع روبوت الدردشة	0.705	0.869
الحاجة للتفاعل البشرى	0.873	0.922
التحكم فى المعلومات	0.747	0.838
الحساسية للمعلومات	0.779	0.871
الأدوات التكنولوجية لدعم الخصوصية	0.836	0.902
مخاوف الخصوصية	0.862	0.906
الإفصاح عن المعلومات	0.699	0.833
التجنب السلوكى	0.879	0.915
الرعاية الأخلاقية التنظيمية للخصوصية	0.700	0.808
Kaiser-Meyer-Olkin. KMO	.892	
Bartlett's	1951.74 (0.000)	
Df	55	

مستوى معنوية ≤ 0.001

المصدر: من اعداد الباحثة اعتماداً على نتائج التحليل الإحصائى لبرنامج SPSS.

تشير نتائج التحليل العاملي الاستكشافي (EFA)، وقيمة معيار Kaiser-Meyer-Olkin (KMO) التي تجاوزت نسبة 50٪، إلى زيادة موثوقية العوامل التي يتم الحصول عليها من التحليل العاملي وكفاية حجم العينة. وهذا يدل على إمكانية استخدام التحليل العاملي للبيانات التي تم جمعها من عينة الدراسة. بالإضافة إلى ذلك، يشير مستوى الدلالة لنتائج اختبار Bartlett عند 0.05 إلى جودة بنود لمقاييس الدراسة ووجود علاقة قوية بين بنود قياس المتغير الواحد.

- اختبار الصدق : باستخدام التحليل العاملى التوكيدى (CFA) Confirmatory Factor Analysis ويمكن توضيح ذلك كما يلى:

- صدق التقارب Convergent Validity

وذلك لقياس مدى التقارب والتوافق بين العبارات التي تقيس المتغير الواحد عن طريق استخدام متوسط التباين المفسر (AVE) Average Variance Extracted ويعد مقبولاً إذا كانت قيمته (0.5) فأكثر، وبناءً على ذلك تشير النتائج الواردة بالجدول (8) إلى أن جميع قيم متوسط التباين المفسر (AVE) تتراوح بين (0.515، 0.798) مما يدل على الصدق التقاربى لمقاييس الدراسة (Hair et al., 2019).

- صدق التمايز Discriminant validity

يشير صدق التمايز إلى أن العبارات المخصصة لقياس متغير ما لا تقيس إلا هذا المتغير فقط، وذلك من خلال قياس مدى التنافر بين متغيرات الدراسة، باستخدام كل من معامل Fornell & Larcker، ومعامل(HTMT).

جدول 8: نتائج الصدق

متغيرات الدراسة	متوسط التباين المفسر (AVE)	القلق التكنولوجى	التجنب السلوكى	التحكم فى المعلومات	الإفصاح عن المعلومات	الألفة مع روبوت الدردشة	الحاجة للتفاعل البشرى	الرعاية الأخلاقية التنظيمية للخصوصية	مخاوف الخصوصية	الأدوات التكنولوجية لدعم الخصوصية	القوانين الحكومية	الحساسية للمعلومات
القلق التكنولوجى	0.543	**0.737**	0.569	-0.092	-0.457	-0.700	0.521	-0.025	0.625	-0.587	0.504	0.546
التجنب السلوكى	0.738	0.713	**0.859**	-0.169	-0.488	-0.491	0.616	-0.077	0.730	-0.725	0.477	0.654
التحكم فى المعلومات	0.565	0.127	0.197	**0.752**	0.039	0.113	-0.132	0.034	-0.177	0.116	-0.108	-0.074
الإفصاح عن المعلومات	0.625	0.638	0.623	0.106	**0.791**	0.348	-0.366	0.118	-0.430	0.486	-0.471	-0.638
الألفة مع روبوت الدردشة	0.769	**0.902**	0.611	0.157	0.498	**0.877**	-0.460	0.023	-0.554	0.504	-0.438	-0.452
الحاجة للتفاعل البشرى	0.798	0.659	0.701	0.157	0.465	0.577	**0.893**	-0.072	0.590	-0.522	0.570	0.558
الرعاية الأخلاقية	0.515	0.079	0.103	0.132	0.164	0.060	0.107	**0.717**	-0.078	0.026	-0.124	-0.056
مخاوف الخصوصية	0.706	0.773	0.830	0.214	0.551	0.699	0.678	0.103	**0.840**	-0.578	0.392	0.637
الأدوات التكنولوجية	0.754	0.759	0.847	0.146	0.637	0.655	0.610	0.052	0.678	**0.868**	-0.443	-0.610
القوانين الحكومية	0.665	0.685	0.588	0.136	0.648	0.594	0.703	0.183	0.483	0.559	**0.815**	0.474
الحساسية للمعلومات	0.693	0.718	0.786	0.097	0.868	0.603	0.675	0.082	0.771	0.755	0.621	**0.833**

قيم القطر المظلل تعبر عن قيم الجذر التربيعى لمتوسط التباين المفسر(AVE)

تعبر القيم أسفل القطر المظلل عن نتائج صدق التمايز باستخدام HTMT <0.9

تعبر القيم أعلى القطر المظلل عن نتائج صدق التمايز باستخدام Fornell & Larcker

المصدر: من اعداد الباحثة اعتماداً على نتائج برنامج Smart -PLS.

ويتضح من الجدول (8) أن قيمة معامل الإرتباط بين أى اثنين من المتغيرات أقل من الجذر التربيعى لمتوسط التباين المفسر (AVE)، وقد تراوحت قيم الإرتباط بين أى متغيرين معاً بين(-0.725، 0.654)، وهى أقل من قيمة معامل Fornell & Larcker، والتي تراوحت بين (0.717، 0.893) ويشير ذلك إلى أن قيم علاقة الإرتباط للمتغيرات مع نفسها أكبر من قيم الإرتباط بين متغير وأخر مما يدل على أن المقاييس المستخدمة فى الدراسة تتصف بدرجة عالية من صدق التمايز (Fornell & Larcker, 1981). كما يتضح أيضاً صدق التمايز من خلال جدول (4) حيث تراوحت قيم معاملات متغيرات الدراسة بين (0.409، 0.726) وهى جميعها أقل من معامل (HTMT) الذى يجب ألا يتجاوز (0.9)فيما عدا قيمة واحدة (0.936)، ويمكن قبول قيمة معامل الارتباط بين أى أثنين من المتغيرات أكثر من (0.9) إذاكانت المفاهيم متشابهة (Sarstedt, Hair & Ringle, 2023)، وبالنظر إلى المتغيرات وجد أن القيمة تنحصر بين متغيرين (القلق التكنولوجى، الألفة مع روبوت الدردشة).

ونتيجة لعدم التشابه بين المتغيرات فقد قامت الباحثة بحذف بند Q17 لمتغير الألفة مع روبوت الدردشة من أجل التحسين، لتصبح القيمة (0.902)، ويعتبر قيمة معامل HTMT معياراً أكثر صرامة ويتطلب فصلاً أكثر وضوحاً بين المتغيرين المختلفين (Henseler, Ringle & Sarstedt, 2015).

(9-5-2) تقييم النموذج الهيكلى

يستخدم تقييم النموذج الهيكلى للحكم على مدى ملاءمة النموذج المقترح لإختبار فروض الدراسة، وقبل اختبارها يجب التأكد من مدى اعتدالية البيانات، وذلك باستخدام معاملى الإلتواء والتفرطح فى الجدول (9)، الذى يوضح أن جميع متغيرات الدراسة تنحرف في توزيعها عن التوزيع الطبيعي فى ضوء الحدود المسموح بها، وعدم إنحرافها عن التوزيع الطبيعي بشكل كبير، حيث تنحصر قيمة "z" المقبولة لكل من معامل التفرطح والإلتواء بين (-2,58، +2,58) عند مستوى معنوية أقل من (0.5)(Hair et al., 2014).

جدول9: اختباراعتدالية البيانات باستخدام الإلتواء والتفرطح

المتغيرات / الإختبارات	التشريعات والقوانين الحكومية	القلق التكنولوجى	الألفة مع روبوت الدردشة	الحاجة للتفاعل البشرى	التحكم فى المعلومات	الحساسية للمعلومات	الأدوات التكنولوجية لدعم الخصوصية	مخاوف الخصوصية	الافصاح عن المعلومات	التجنب السلوكى	الرعاية الأخلاقية التنظيمية للخصوصية
معامل الالتواء	-.700	-.186	-.253	.677	-.576	-.505	.038	-.252	.343	-.049	-.811
معامل التفرطح	.219	-.055	-.191	.086	.509	.031	-.315	-.149	-.149	-.382	-.212

المصدر: من اعداد الباحثة اعتماداً على نتائج التحليل الإحصائى ببرنامج SPSS.

كما يجب التأكد من عدم وجود ازدواج خطي Multicollinearity بين المتغيرات المستقلة قبل القيام باختبار الفروض، وذلك باستخدام معامل التضخم المتباين Variance Inflation Factor (VIF) والذى يتراوح بين (1، 2.505) بالجدول (10).

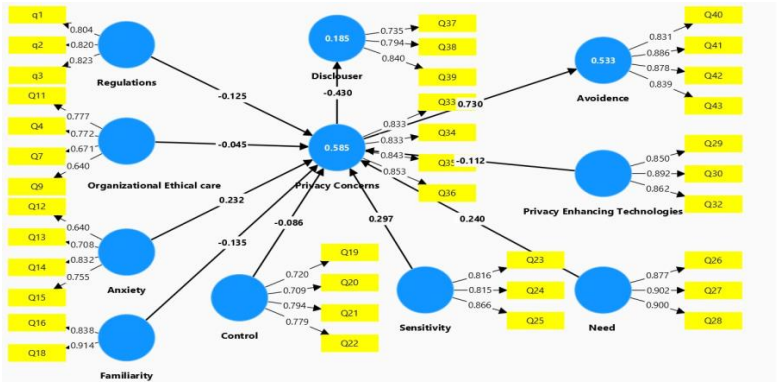
جدول10: اختبار التعددية الخطية - معامل تضخم التباين (VIF)

المتغيرات	مخاوف الخصوصية	التجنب السلوكى	الافصاح عن للمعلومات
الأدوات التكنولوجية لدعم الخصوصية	1.956		
التحكم فى المعلومات	1.026		
التشريعات والقوانين الحكومية	1.685		
الرعاية الأخلاقية التنظيمية للخصوصية	1.119		
القلق التكنولوجى	2.505		
الحاجة للتفاعل البشرى	1.896		
مخاوف الخصوصية		1.000	1.000
الألفة مع روبوت الدردشة	2.055		
الحساسية للمعلومات	1.931		

المصدر: من اعداد الباحثة اعتماداً على نتائج برنامج Smart -PLS .

وهو أقل من الحد الأقصى (10) كما أنه يقع فى الحدود المقبولة لكل متغيرين مستقلين معاً والذى يجب أن يتراوح بين (0.2، 5) وهو ما يوضح عدم وجود ازدواج خطي بين المتغيرات المستقلة، ومن ثم يمكن الإستمرار فى اختبار فروض الدراسة (Hair et al., 2010; Pallant, 2016).

ويوضح الشكل رقم (2) نموذج القياس المحسن الذى تم تطويره لقياس متغيرات الدراسة تمهيداً لإختبار الفروض، وقامت الباحثة بحذف البنود (Q5،Q6،Q8،Q10) من متغيرالرعاية الأخلاقية التنظيمية للخصوصية، وأيضاً حذف البند (Q31) من متغير الأدوات التكنولوجية لدعم الخصوصية، وذلك من أجل التحسين.



شكل 3: نموذج القياس

يوضح جدول (11) من واقع نموذج القياس السابق النتائج الإحصائية لطريقة المربعات الصغرى الجزئية للنموذج الهيكلى، والتي تتمثل فى معامل التفسير R^2، والذى يعبر عن المعيار الرئيسى لتقييم نموذج القياس والحكم على القدرة التنبؤية لنموذج الدراسة وتشير قيمة معامل التفسير التي تساوي 0.25 أو 0.5 أو 0.75 إلى قدرة تنبؤية ضعيفة أو متوسطة أو قوية على التوالى (Hair et al., 2014).

يفسر نموذج القياس المحسن التغير في مخاوف الخصوصية بنسبة 58.4%، ثم التجنب السلوكى بنسبة 53.3 % وهى نسب تعد متوسطة، فى حين أن نسبة التفسير للإفصاح عن المعلومات كانت بنسبة 18.5%، وهى نسبة ضعيفة.

جدول 11: معاملات التفسير لنموذج الدراسة

معامل التفسير	التجنب السلوكى	الإفصاح عن المعلومات	مخاوف الخصوصية
R^2	0.533	0.185	0.584

المصدر: من اعداد الباحثة اعتماداً على نتائج برنامج Smart -PLS

تظهر النتائج فى جدول (12) أن 9 فروض من أصل 10 تم قبولها عند مستويات معنوية مختلفة ويمكن توضيح نتائج اختبار الفروض على النحو التالى:

الفرض الأول ف1: يؤثر القلق التكنولوجى عند استخدام روبوت الدردشة تأثيراً إيجابياً على شعور العملاء بمخاوف الخصوصية.

يتبين من النتائج وجود تأثير إيجابى ذو دلالة إحصائية، بين قلق العملاء عند استخدام روبوت الدردشة ومخاوف الخصوصية حيث بلغت قيمة β (0.232)، وقيمة ت (3.523) عند مستوى معنوية أقل من 0.001، وهو ما يفسر قبول الفرض الأول.

الفرض الثانى ف2: تؤثر الألفة مع روبوت الدردشة تأثيراً سلبياً على شعور العملاء بمخاوف الخصوصية.

يتبين من النتائج وجود تأثير سلبى ذو دلالة إحصائية بين الألفة مع روبوت الدردشة ومخاوف الخصوصية، حيث بلغت قيمة β (-0.135) وقيمة ت (2.354) عند مستوى معنوية أقل من 0.05، وهو ما يفسر قبول الفرض الثانى.

الفرض الثالث ف3: يؤثر إدراك العملاء للتحكم فى المعلومات تأثيراً سلبياً على شعورهم بمخاوف الخصوصية.

تشير النتائج إلى وجود تأثير سلبى ذو دلالة إحصائية بين إدراك العملاء للتحكم فى المعلومات ومخاوف الخصوصية، حيث بلغت قيمة β (-0.086) وقيمة ت (2.777) عند مستوى معنوية أقل من 0.01. وهو ما يفسر قبول الفرض الثالث.

الفرض الرابع ف4: تؤثر حساسية العملاء للمعلومات تأثيراً إيجابياً على شعورهم بمخاوف الخصوصية.

يتبين من النتائج وجود تأثير إيجابى ذو دلالة إحصائية بين حساسية العملاء للمعلومات ومخاوف الخصوصية، حيث بلغت قيمة β (0.297) وقيمة ت (5.957) عند مستوى معنوية أقل من 0.001. وهو ما يفسر قبول الفرض الرابع.

الفرض الخامس ف5: يؤثر توافر القوانين والتشريعات الحكومية لحماية الخصوصية تأثيراً سلبياً على شعور العملاء بمخاوف الخصوصية.

يتبين من النتائج وجود تأثير سلبى ذو دلالة إحصائية بين توافر التشريعات الحكومية لحماية مستخدمى روبوتات الدردشة ومخاوف الخصوصية، حيث بلغت قيمة β (0.125-) وقيمة ت (2.747) عند مستوى معنوية أقل من 0.01، وهو ما يفسر قبول الفرض الخامس.

الفرض السادس ف6: تؤثر الرعاية الأخلاقية البنكية للخصوصية تأثيراً سلبياً على شعور العملاء بمخاوف الخصوصية.

أكدت النتائج على عدم وجود تأثير للرعاية الأخلاقية البنكية للخصوصية ومخاوف الخصوصية، حيث بلغت قيمة β (0.045-) وقيمة ت (0.962) عند مستوى معنوية 0.336. وهو ما يفسر رفض الفرض السادس.

الفرض السابع ف7: تؤثر حاجة العملاء للتفاعل البشرى تأثيراً إيجابياً على شعورهم بمخاوف الخصوصية.

يتبين من النتائج وجود تأثير إيجابى ذو دلالة إحصائية بين حاجة العملاء للتفاعل البشرى ومخاوف الخصوصية، حيث بلغت قيمة β (0.240) وقيمة ت (4.549) عند مستوى معنوية أقل من 0.05. وهو ما يفسر قبول الفرض السابع.

الفرض الثامن ف8: يؤثر توافر الأدوات التكنولوجية لدعم الخصوصية تأثيراً سلبياً على شعور العملاء بمخاوف الخصوصية.

يتبين من النتائج وجود تأثيراً سلبياً ذو دلالة إحصائية بين توافر الأدوات التكنولوجية لحماية الخصوصية ومخاوف الخصوصية، حيث بلغت قيمة β (0.112-) وقيمة ت (2.082) عند مستوى معنوية أقل من 0.001. وهو ما يفسر قبول الفرض الثامن.

الفرض التاسع ف9: يؤثر شعور العملاء بمخاوف الخصوصية من استخدام روبوت الدردشة تأثيراً إيجابياً على التجنب السلوكى.

يتبين من النتائج وجود تأثير إيجابى ذو دلالة إحصائية بين شعور العملاء بمخاوف الخصوصية من استخدام روبوت الدردشة والتجنب السلوكى، حيث بلغت قيمة β (0.730) وقيمة ت (24.186) عند مستوى معنوية أقل من 0.001، وهو ما يفسر قبول الفرض التاسع.

الفرض العاشر ف10: يؤثر شعور العملاء بمخاوف الخصوصية من استخدام روبوت الدردشة تأثيراً سلبياً على الإفصاح عن المعلومات.

تشير النتائج إلى وجود تأثير سلبى ذو دلالة إحصائية بين شعور العملاء بمخاوف الخصوصية من استخدام روبوت الدردشة والإفصاح عن المعلومات ، حيث بلغت قيمة β (0.430-) وقيمة ت (9.172) عند مستوى معنوية أقل من 0.001. وهو ما يفسر قبول الفرض العاشر.

جدول 12: نتائج إختبار فروض الدراسة

	فروض الدراسة	التأثير	بيتا(β)	ت المحسوبة	درجة المعنوية	النتيجة
ف1	القلق التكنولوجى -> مخاوف الخصوصية	(+)	0.232	3.523	0.000	قبول***
ف2	الألفة مع روبوت الدردشة -> مخاوف الخصوصية	(-)	-0.135	2.354	0.019	قبول*
ف3	التحكم فى المعلومات -> مخاوف الخصوصية	(-)	-0.086	2.777	0.006	قبول**
ف4	حساسية المعلومات -> مخاوف الخصوصية	(+)	0.297	5.957	0.000	قبول***
ف5	القوانين الحكومية -> مخاوف الخصوصية	(-)	-0.125	2.747	0.006	قبول**
ف6	الرعاية الأخلاقية للخصوصية -> مخاوف الخصوصية	(-)	-0.045	0.962	0.336	رفض
ف7	الحاجة للتفاعل البشرى-> مخاوف الخصوصية	(+)	0.240	4.549	0.000	قبول***
ف8	الأدوات التكنولوجية لدعم الخصوصية -> مخاوف الخصوصية	(-)	-0.112	2.082	0.037	قبول*
ف9	مخاوف الخصوصية -> التجنب السلوكى	(+)	0.730	24.186	0.000	قبول***
ف10	مخاوف الخصوصية -> الإفصاح عن المعلومات	(-)	-0.430	9.172	0.000	قبول***

*قبول الفرض عن مستوى معنوية ≤ 0.05 ، ** قبول الفرض عند مستوى معنوية ≤ 0.01 ، *** قبول الفرض عند مستوى معنوية ≤ 0.001

المصدر: من اعداد الباحثة اعتماداً على نتائج برنامج Smart- PLS .

(10) مناقشة نتائج الدراسة

تهدف هذه الدراسة، إلى دراسة العوامل المؤثرة على مخاوف الخصوصية ونتائجها السلوكية بين عملاء البنوك مستخدمى روبوت الدردشة فى الخدمة البنكية، وذلك بدمج إطارين نظريين هما نظرية "التنمية متعددة الأبعاد" (MDT)، ونموذج "المسببات- مخاوف الخصوصية -النتائج" (APCO). توفر الدراسة فهماً أكثر دقة للمسببات والنتائج الإيجابية والسلبية لمخاوف الخصوصية، وأظهرت النتائج أن العوامل الأربعة المحددة فى الدراسة لها تأثيرات مباشرة وتفاعلية بدرجات متفاوتة على مخاوف الخصوصية لدى العملاء مستخدمى روبوت الدردشة فى الخدمة البنكية. وأن العملاء لديهم مستوى متوسط من مخاوف الخصوصية، ويدل ذلك على أن العملاء في الدول النامية لديهم اهتمام بالخصوصية مثل العملاء في أنحاء أخرى من العالم.

وهذا يكسر الصورة النمطية القائلة بأن العملاء في البلدان النامية أقل اهتماماً بالخصوصية مقارنة بالدول المتقدمة، وهذا يمثل إنذاراً للممارسين في المجال البنكى لعدم استغلال المعلومات الشخصية للعملاء. كما توضح الدراسة أن مستوى مخاوف الخصوصية يرتبط بالعديد من العوامل منها البيئية والفردية كما يعتمد على مدى التفاعل بين الإنسان والتكنولوجيا، وإدارة المعلومات وهو ما يتماشى مع نظرية "التنمية متعدد الأبعاد" التى تقترح أن العوامل التي تؤثر على إدراك المستخدمين لخصوصية المعلومات وغزو الخصوصية Privacy invasion يمكن تقسيمها إلى أربعة أبعاد: البعد البيئي، والفردى، وإدارة المعلومات، وإدارة التفاعل، كما تتفق النتائج مع نموذج "المسببات- مخاوف الخصوصية -النتائج" (APCO)، فيما يتعلق بالعوامل المؤثرة على مخاوف الخصوصية، إضافة إلى النتائج السلوكية المترتبة عليها من تجنب سلوكى وإفصاح عن المعلومات.

(1-10) مناقشة نتائج الدراسة للعوامل المؤثرة على مخاوف الخصوصية

كشفت النتائج عن أدلة داعمة لنظرية "التنمية متعددة الأبعاد" (MDT)، ونموذج "المسببات- مخاوف الخصوصية - النتائج" (APCO)، وتبين أن نسبة كبيرة من هذه الأدلة تُظهر تأثيرات تفاضلية كبيرة على مخاوف الخصوصية مقارنة بالأخرى، ويمكن توضيح ذلك فيما يلي:

- يلعب العامل المرتبط بإدارة المعلومات دوراً هاماً في التأثير على مخاوف الخصوصية. وترتبط بإدارة العملاء لمعلوماتهم الشخصية التي تم إنشاؤها أثناء التفاعل مع روبوت الدردشة للخدمة البنكية. وتعد حساسية المعلومات أقوى دافع لمخاوف الخصوصية مقارنة بجميع المتغيرات المستقلة الأخرى، ويرجع السبب فى ذلك إلى أن المعلومات المطلوبة من روبوتات الدردشة للمواقع البنكية ذات طبيعة حساسة بالنسبة لعينة الدراسة، وذلك كشرط أساسى للتفاعل مع روبوتات الدردشة، ويعزى ذلك إلى الطبيعة الثقافية للمواطنين المصريين الذين يتوخون الحذر بشأن العواقب السلبية للكشف عن معلوماتهم الشخصية، وتتفق هذه النتيجة مع دراسة (Tao et al. 2024; Sun et al. 2023; Jozani et al. 2020).

تشير النتائج أيضاً إلى أن التحكم في المعلومات يعتبر أقوى عامل رادع لمخاوف الخصوصية بين جميع المتغيرات المستقلة. فالعملاء الذين يمتلكون أقل درجة من التحكم في معلوماتهم الشخصية هم الأكثر إحساساً بمخاوف الخصوصية. ينظر العملاء إلى الخصوصية بمدى سيطرتهم على المعلومات الشخصية التي يتم مشاركتها، وطريقة جمعها، والأطراف التي يتشاركون معهم. ومع ذلك، فإن معظم العملاء يفتقرون إلى الوعي الكامل أو يشعرون بالقلق بشأن التحكم في كيفية استغلال بياناتهم الشخصية ومشاركتها مع أطراف أخرى. فعندما يقوم البنك بجمع معلومات شخصية عن العملاء، تُعتبر هذه الممارسة عادلة إذا كان لدى العملاء الوعي الكامل والتحكم في كمية ونوعية المعلومات التى ستستخدم لاحقاً، وذلك وفقاً لنظرية العقد الاجتماعي Social Contract Theory. وفي الحالات التي لا يكون فيها العملاء على دراية كاملة بجمع المعلومات أو استخدامها، أو عندما يكونوا غير قادرين على إلغاء الإشتراك لجمع المعلومات واستخدامها، يمكن أن ينتهك العقد الاجتماعي. فزيادة السيطرة المدركة على المعلومات الشخصية يمكن أن تؤدي إلى رغبة أكبر في مشاركة المعلومات، وعلى الرغم من إدراك العملاء لمخاطر مشاركة المعلومات على مواقع روبوتات الدردشة، إلا أنه قد يكون لديهم شعور زائف بالسيطرة على معلوماتهم. فالتحكم في المعلومات يمثل عاملاً محورياً مهماً في مخاوف الخصوصية، وتتوافق هذه النتيجة مع دراسة كل من (Rodríguez-Priego et al., 2023; Sun et al. 2023; Tseng et al. 2022; Ha et al. 2021).

- يعد العامل المرتبط بالعملاء أمراً بالغ الأهمية في تشكيل مخاوف الخصوصية، وأظهرت النتائج أن الألفة مع روبوتات الدردشة بالنسبة للعملاء الذين لديهم معرفة ولديهم المزيد من الخبرة فى التعامل مع روبوتات الدردشة كان له تأثير سلبي على مخاوف الخصوصية، ومن المرجح أن يكون العملاء مستخدمى روبوتات الدردشة أكثر مهارة في حماية خصوصيتهم ،وبالتالي يكون لديهم نسبة أقل من مخاوف الخصوصية. تشير النتائج إلى أن الألفة مع روبوتات الدردشة، تؤدي إلى مخاوف أقل من الخصوصية، وذلك يدل على أن عينة الدراسة تتمتع بالألفة مع روبوتات الدردشة الذى يعتبر أحد الجوانب الهامة لشعورهم بالراحة. مما يبرز أهمية تلبية احتياجات العملاء في تصميم الروبوتات لتحقيق أقصى درجات الراحة والثقة. وتتوافق هذه النتيجة مع دراسة كل من (Söderlund et al.2022; Ashfaq et al. 2020).

وبالنظر إلى الأسباب الفردية لمخاوف الخصوصية، أظهرت النتائج أن القيمة التي يضعها المستخدمون للقلق التكنولوجى من استخدام روبوتات الدردشة تؤثر بقوة على ادراكهم لمخاوف الخصوصية، وهو ما يتماشى مع نظرية التنمية متعددة الأبعاد على وجه التحديد. إن تأثير القلق التكنولوجي على مخاوف الخصوصية يمكن أن يؤدي إلى الإرتباك ويجعل العملاء

يشعرون بعدم الإرتياح. ويتضح ذلك من إجابات عينة الدراسة حيث أظهر المشاركون درجة عالية من القلق التكنولوجى، ونظراً لأن الخدمة البنكية معقده بطبيعتها، لذلك فمن المتوقع شعور العملاء بالقلق والرهبه من التعامل مع التكنولوجيا البنكية، وخاصة عند التفاعل مع روبوتات الدردشة. فعندما يشعر العملاء بالقلق التكنولوجي، فإنهم يصدرون أحكاماً أكثر تشاؤماً بشأن النتائج المحفوفة بالمخاطر. ويتضح من نتائج الدراسة أن التفاعل مع روبوتات الدردشة يؤدى إلى مشاعر مخيفة بين هؤلاء العملاء الذين يشعرون بمزيد من القلق عند استخدام هذه التكنولوجيا. وتتوافق هذه النتيجة مع دراسة كل من (Inan et al. 2022; Anic et al. 2019; Skrinjaric et al. 2018).

- دور العوامل البيئية فى التأثير على مخاوف الخصوصية، تشمل العوامل البيئية فى الدراسة الحالية كل من العوامل الخارجية الرسمية مثل توافر القوانين والتشريعات الحكومية لحماية الخصوصية، والعوامل الداخلية التنظيمية غير الرسمية مثل الرعاية الأخلاقية البنكية للخصوصية.

أظهرت النتائج أن العوامل البيئية الخارجية تؤثر سلبياً على شعور العملاء بمخاوف الخصوصية، ويدل ذلك على أنه إذا كانت اللوائح والقوانين مصاغة بشكل سليم وتُمكن العملاء من الخصوصية، فإنه يعزز من ثقتهم في أمان بياناتهم الشخصية. وبالتالي، يُمكن لهؤلاء العملاء التعبير عن بياناتهم بثقة عند التفاعل مع روبوت الدردشة، خاصة إذا كانت هناك آليات تمكّنهم من المطالبة بحقوقهم فى الخصوصية. ومن الجدير بالذكر أن اعتقاد العملاء بأن القوانين تمنحهم سلطة في فرض عقوبات على المنتهكين لخصوصيتهم يزيد من إيمانهم بأهميتها، ويؤدى إلى تخفيض مخاوف الخصوصية التى قد يشعر بها العملاء فى غياب القوانين الحكومية الرسمية لحماية بياناتهم الشخصية. وبما أن العملاء في عالم الإنترنت غالباً ما يجدون أن التوازن في جمع واستخدام المعلومات مائلاً لصالح المؤسسات، فإن القوانين تلعب دوراً حيوياً في إيجاد توازن القوى بين الأفراد والمؤسسات العامة والخاصة. وهذا يشير إلى أهمية كبيرة لتوفير قوانين تعزز الثقة بين الأفراد وتنظم جمع واستخدام المعلومات الشخصية بشكل مناسب، مما يعزز حماية الخصوصية. فالعملاء الذين يثقون في أن القوانين تضمن حماية الخصوصية وتنظم جمع واستخدام المعلومات الشخصية أقل قلقاً بشأن احتمالية انتهاك الخصوصية. وهذا يتماشى مع نظرية التنمية متعددة الأبعاد التي تشير إلى أن القوانين تلعب دوراً مهماً في تقليل المخاوف والقلق. وتتوافق هذه النتيجة مع دراسة كل من (Khan 2024; Khoury et al. 2023; Bano et al. 2022).

على عكس مقترحات نظرية التنمية متعددة الأبعاد والأبحاث السابقة، لم تظهر نتائج الدراسة تأثيراً للعوامل البيئية الداخلية غير الرسمية - الرعاية الأخلاقية البنكية - على مخاوف الخصوصية، على الرغم من أن المستجيبين يظهرون إدراكهم للرعاية الأخلاقية البنكية للخصوصية بدرجة متوسطة إلا أنها لم تخفض من مخاوف الخصوصية لديهم.

قد يعود السبب في ذلك إلى أن العملاء رغم تقديرهم للرعاية الأخلاقية التى توفرها البنوك للخصوصية، إلا أنهم لم يغيروا مشاعر الخوف من انتهاك الخصوصية عند استخدام روبوتات الدردشة بمجرد تلقيهم لتلك الفوائد. فعندما يشعر العملاء بأن البنوك تحترم وتحمى خصوصيتهم، فإن ذلك يشعرهم بالأمان ويزيد من ثقتهم بدلاً من تقليل مخاوفهم بشأن الخصوصية. وقد تختلف العلاقة بين الرعاية الأخلاقية للخصوصية في البنوك ومخاوف الخصوصية باختلاف الثقافات. فما يشكل الرعاية الأخلاقية لبيئة ثقافية، قد لا يُدرك بنفس الطريقة في بيئة أخرى. لذلك، قد لا يكون من المنطقي تعميم العلاقة السلبية بناءً على بيئة محددة. بالإضافة إلى ذلك، قد تعزز البرامج الإعلامية والحوار العام حول قضايا الخصوصية في مصر مخاوف الخصوصية، مما يغطي أي جهود تبذلها البنوك لإظهار الرعاية الأخلاقية. وتتعارض هذه النتيجة مع دراسة كل من (Mattison Thompson & Siamagka 2022; Singh et al. 2020).

- دور إدارة التفاعل فى التأثير على مخاوف الخصوصية. على الرغم من أن تفضيل التفاعل بين الإنسان والآلة يختلف وفقاً للصناعة، إلا أن نتائج الدراسة تتفق مع العديد من الدراسات التى تم تطبيقها على صناعات أخرى مثل الخدمات

الإلكترونية (Ashfaq et al., 2020)، التأمين(Rajaobelina et al., 2021). تشير النتائج إلى أن العملاء يفضلون التفاعل مع الخبراء البشريين مقارنة ببرامج الدردشة الآلية. هذا يدل على أن العملاء الذين يفضلون التفاعل مع وكلاء الخدمة البشريين يشعرون بعدم الراحة والقلق عند التعامل مع البرامج الآلية. فالعملاء الذين يحتاجون إلى تفاعل إنساني يرون أن التفاعل مع البشر أكثر موثوقية ومتعة وسهولة مقارنة بالتفاعل مع الآلات. قد يكون السبب في ذلك جزئياً هو عدم قدرة البرامج الآلية على تقديم استجابات مشابهة لتلك التي يقدمها البشر، حيث تعتمد روبوتات الدردشة البنكية بشكل أساسي على النصوص. في هذه الحالة، يشعر العملاء بالقلق أو الإضطراب بدلاً من الراحة. ويتغير التفاعل الإنساني مع الروبوتات بناءً على مدى تشابهها مع البشر، مما يعني أن الروبوتات التي تقترب من التشابه مع البشر جزئياً تثير مشاعر سلبية، حتى تصل إلى مرحلة من التشابه الكامل حيث يزداد القبول والراحة مرة أخرى.

قد يكون للعملاء الذين يفضلون التفاعل البشري ثقة أكبر في التعامل مع البشر مقارنةً بالروبوتات. هؤلاء العملاء يشعرون بأن مشاركة معلوماتهم الشخصية مع البشر أكثر أماناً. بالإضافة إلى ذلك، فإن هؤلاء العملاء قد يعانون من مخاوف متزايدة تتعلق بالخصوصية عند استخدام الروبوتات في الخدمات المالية، خوفاً من انتهاك خصوصيتهم أو إساءة استخدام معلوماتهم الشخصية. هذه النتيجة تتوافق مع دراسة كل من (Rhim et al.2024; Ischen et al.2020; Følstad et al. 2018) .

أشارت النتائج إلى وجود تأثير سلبي بين إدراك العملاء لتوافر أدوات تكنولوجية لحماية ودعم الخصوصية وشعورهم بمخاوف الخصوصية. تشمل هذه الأدوات تشفير البيانات، جدران الحماية، تكنولوجيا البصمة الحيوية. مما يجعل فك رموزها من قبل المتسللين واستخدامها بطرق غير مصرح بها أمراً صعباً، بالإضافة إلى وجود سياسات الخصوصية التي توفر معلومات دقيقة حول كيفية جمع البيانات واستخدامها ومشاركتها. كما تشمل الإجراءات المتبعة لحماية الخصوصية أيضاً التحقق المزدوج لتأكيد هوية المستخدم وحماية بياناته الشخصية، يؤدى ذلك إلى تعزيز ثقة المستخدمين وتقليل مخاوفهم بشأن الخصوصية عند استخدام روبوتات الدردشة في الخدمة البنكية. تتوافق هذه النتيجة مع دراسة كل من (Khan 2024; Hariri 2023; Sebastian 2023) .

(10-2) مناقشة النتائج السلوكية المترتبة على مخاوف الخصوصية

تشير النتائج إلى أن العملاء يظهرون مستوى متوسط من التجنب السلوكي، وتلعب المشاعر السلبية مثل مخاوف الخصوصية دوراً هاماً في هذا السلوك. ويتضح ذلك من نظرة العملاء إلى روبوتات الدردشة على أنها تطفل على خصوصيتهم وتقييد لحريتهم الشخصية، مما يدفعهم لمحاولة استعادة تلك الحرية من خلال التجنب السلوكي. يعني ذلك أنه إذا زادت مخاوف العملاء بشأن الخصوصية عند استخدام روبوتات الدردشة في الخدمات البنكية، فإن ذلك سيؤثر سلبياً على ثقتهم فى حماية البنوك لهذه المعلومات. ويؤدي ذلك إلى قيام العملاء بمجموعة من السلوكيات مثل صرف الانتباه عن روبوت الدردشة أو تجاهله عن عمد، مثل النظر بعيداً أو التمرير عبر محتوى آخر على الموقع البنكي، أو النقر بعيداً بمجرد ظهور روبوت الدردشة. قد يصل الأمر إلى إغلاق الموقع البنكي بشكل متعمد للحد من جمع البيانات عبر الإنترنت من خلال خاصية التتبع. هذه النتائج تتوافق مع دراسة كل من (Wang et al. 2024; Jain & .Purohit 2022; Singaraju et al. 2022; Aiolfi et al. 2021) .

أظهرت الدراسة وجود علاقة سلبية بين مخاوف الخصوصية واستعداد العملاء للإفصاح عن معلوماتهم. فكلما زادت مخاوف العملاء من التعرض لانتهاك خصوصيتهم، كلما قلت رغبتهم في الكشف عن المعلومات الشخصية.

ويتفق ذلك مع "مفارقة الخصوصية "privacy paradox"، فإن مخاطر الخصوصية المدركة لا تترجم تلقائياً إلى عدم الكشف عن المعلومات أو التجنب، ولكن قد يعرب العملاء عن مخاوفهم بشأن خصوصيتهم باستخدام روبوتات الدردشة،

ولكنهم ينخرطون لاحقاً في سلوكيات يقدمون فيها معلومات حساسة إذا كانوا يعتقدون أنهم سيحصلون على شيء ما في المقابل. لذلك لا يحمون خصوصيتهم كما هو متوقع ويتم ذلك فى تقييم الأحداث قصيرة الأجل بشكل مختلف عن الأحداث طويلة الأجل، هذا يعني أن مزايا الكشف عن المعلومات الحساسة يمكن ملاحظتها بسهولة على المدى القصير، ولكن مخاطر القيام بذلك قد تكون غير مرئية أو يُنظر إليها على أنها تحدث على المدى الطويل. قد يكون السبب الذى يدفع المستخدمين للافصاح هو نتائج تقييم المخاطر والفوائد، ويرى العملاء أن الفوائد تتجاوز المخاطر. وبما أن المحادثة مع برنامج الدردشة الآلى ظاهرة جديدة إلى حد ما، فقد يكون العملاء أكثر وعياً بالطلبات المباشرة للكشف عن المعلومات، مما يؤدي إلى المزيد من المخاوف المتعلقة بالخصوصية. وتؤثر المخاوف المتعلقة بالخصوصية سلبياً على الإفصاح عن المعلومات، فكلما كانت المخاوف من الخصوصية أعلى، كلما كان الإفصاح عن المعلومات الشخصية أقل، وبالتالي كانت احتمالية التعامل مع روبوتات الدردشة أقل. وتتوافق هذه النتيجة مع دراسة كل من (Le et al. 2024; Roozen et al. 2022; Ischen et al. 2020).

(11) توصيات الدراسة

تقدم الدراسة مجموعة من التوصيات يمكن عرضها فى الجدول (13) كما يلى:

جدول 13: خطة عمل ارشادية لتنفيذ توصيات الدراسة

التوصية	آلية التنفيذ	الجهة المسئولة عن التنفيذ
يجب على المشرعين وصانعى السياسات صياغة إطار قانوني مناسب لحماية خصوصية بيانات عملاء البنوك مستخدمى روبوتات الدردشة بشكل كاف وفعال، كما ينبغي أن يضمن هذا الإطار التنفيذ السليم للقوانين، مما يساعد المستخدمين على الثقة في أمان بياناتهم الشخصية.	- صياغة وسن التشريعات والقوانين محكمة وشاملة تغطي جميع جوانب حماية البيانات، وتضمن إرشادات واضحة لجمع البيانات وتخزينها ومشاركتها، وذلك بالتشاور مع الخبراء في مجال القانون والأمن السيبراني. - ضمان التنفيذ السليم وذلك بإنشاء هيئة مسئولة عن مراقبة وتنفيذ قوانين الخصوصية، والعمل على المراجعة الدورية لضمان الالتزام بها . - تشكيل لجنة لمراجعة وتحديث قوانين الخصوصية باستمرار لمواكبة التطورات التكنولوجية. - رفع الوعي من خلال إطلاق حملات توعية عامة لتثقيف المواطنين حول حقوقهم في الخصوصية وأهمية حماية البيانات الشخصية، على المواقع الإلكترونية للبنوك وغيرها من المؤسسات المالية.	**التنسيق بين كل من المشرعين وصانعى السياسات والخبراء فى القانون فى الحكومة المصرية، وإدارات البنوك المتمثلة فى كل من إدارة الشئون القانونية، إدارة تكنولوجيا المعلومات.**
ينبغي إضافة خصائص بشرية مجسمة لروبوتات الدردشة لجعل العملاء يشعرون بالاهتمام والرعاية، والنظر إليها على أنها كيانات اجتماعية وليست مجرد آلات، مما يعزز شعور العملاء بالإهتمام.	- تصميم روبوت الدردشة ليظهر كمساعد "خدمة ودود"، من خلال برمجة الروبوت ليقدم التحيات الأولية والبيانات بشكل يحاكى لغة البشر. - إضافة خصائص تجعل الروبوت يخاطب العملاء بشكل شخصي ويوفر لهم الراحة العاطفية والتشجيع. - إضافة مهارات التواصل الإنساني، وذلك بتمكين الروبوت من بدء محادثات صغيرة مع العملاء، مثل الاستفسار عن أحوالهم أو تقديم نصائح بسيطة. - تصميم الروبوت ليظهر قدرة عقلانية في حل المشكلات بشكل يوحي بالكفاءة والثقة .	**التنسيق بين إدارت البنك المختلفة مثل إدارة تكنولوجيا المعلومات، إدارة التسويق والعلاقات العامة، ومصممى روبوتات الدردشة.**
يجب على مصممي روبوتات الدردشة فى الخدمة البنكية تحقيق توازن دقيق بين حساسية المعلومات التي تطلبها المواقع وبين الخدمات والمزايا المقدمة في المقابل.	- تقليل طلب المعلومات الحساسة من خلال مراجعة نماذج جمع البيانات وتحديد المعلومات الأساسية الضرورية فقط، حذف أي حقول غير ضرورية تتعلق بالمعلومات الحساسة. - توضيح سبب طلب المعلومات من خلال شرح واضح ومفصل عن سبب طلب كل نوع من المعلومات الشخصية. واستخدام نصوص تفاعلية وأدوات توضيحية لشرح الفوائد الناتجة من توفير المعلومات.	**التنسيق بين مصممى روبوتات الدردشة، إدارة تكنولوجيا المعلومات والأمن السيبرانى.**

يجب على البنوك الالتزام بالعقد الاجتماعي الضمني مع العملاء لتجنب التجارب السلبية الناتجة عن انتهاك الخصوصية. يجب أيضاً اتخاذ الحيطة عند تحويل ملفات المشتركين وتزويد بياناتهم لأطراف ثالثة.	- الالتزام بالعقد الاجتماعي الضمني من خلال تطوير سياسات خصوصية واضحة وشفافة توضح كيفية جمع البيانات واستخدامها ومشاركتها. وتقديم ضمانات لاستخدام البيانات الشخصية للعملاء فقط للأغراض المتفق عليها. - حماية البيانات عند التحويل وذلك باستخدام أدوات تشفير قوية عند نقل ملفات المشتركين لضمان عدم تسريب البيانات، واجراء فحص دقيق للأطراف الثالثة لضمان التزامهم بسياسات الخصوصية والأمان. - تضمين أدوات مكافحة الاحتيال في روبوتات الدردشة لتوفير حماية إضافية.	**التنسيق بين الإدارة التنفيذية للبنك، إدارة تكنولوجيا المعلومات والأمن السيبراني، إدارة خدمة العملاء.**
يجب على القائمين على المواقع البنكية أن يكونوا على دراية بالآثار المحتملة لمخاوف الخصوصية. تنفيذ سياسة خصوصية واضحة وموجزة، وزيادة الشفافية بشأن البيانات التي يتم جمعها واستخدامها.	- معرفة الآثار المحتملة لمخاوف الخصوصية من خلال تدريب الموظفين للتعرف على تأثير مخاوف الخصوصية على سلوك العملاء. - إجراء بحوث واستقصاءات دورية لقياس مخاوف العملاء واستجابتهم لسياسات الخصوصية. - تزويد العملاء بالأدوات اللازمة للتحكم فى البيانات، وتوفير أدوات رقمية تساعد العملاء في مراقبة وحماية بياناتهم الشخصية. وتقديم الدعم الفني للعملاء حول كيفية استخدام هذه الأدوات بفعالية. - إنتاج مقاطع فيديو ونصوص توضيحية تشرح كيفية عمل روبوتات الدردشة ودور المعلومات المطلوبة. وتوفير ورش عمل ودورات تدريبية للعملاء حول كيفية حماية بياناتهم الشخصية على الإنترنت.	**التنسيق بين إدارة تكنولوجيا المعلومات، إدارة التسويق والعلاقات العامة، إدارة الموارد البشرية، إدارة الدعم الفني وخدمة العملاء.**
ضرورة المشاركة المستمرة مع العملاء في الأمور المتعلقة بالتطفل على الخصوصية وتعزيز الحوار بين البنوك والعملاء، من خلال إنشاء منتدى مفتوح عبر الإنترنت، أو خط هاتفي ساخن مباشر، للاستجابات النشطة والسريعة.	- تطوير منتدى تفاعلي على موقع البنك الإلكتروني يسمح للعملاء بمناقشة مخاوف الخصوصية وتقديم اقتراحاتهم. - تعيين مشرفين متخصصين للرد على الاستفسارات وضمان تنظيم الحوار بشكل فعّال. - تقديم جلسات حوارية دورية مع خبراء الأمن السيبراني لمناقشة القضايا الحالية والإجابة على أسئلة العملاء. - إطلاق خط هاتفي ساخن مخصص لاستقبال مكالمات العملاء المتعلقة بمخاوف الخصوصية.	**التنسيق بين إدارة تكنولوجيا المعلومات، إدارة الموارد البشرية، إدارة الدعم الفني وخدمة العملاء.**

(12) حدود الدراسة والدراسات المستقبلية

على الرغم من أن الدراسة الحالية تقدم نتائج هامة، إلا أنها تتضمن بعض القيود التى لا تنتقص من أهمية النتائج المحققة، لكنها تبرز عدة قضايا تستدعي المزيد من البحث كمجالات محتملة للدراسات المستقبلية، والتى يمكن توضيحها كما يلى:

- على الرغم من أن الدراسة سيطرت على العديد من المتغيرات المؤثرة على مخاوف الخصوصية، إلا أن القوة التفسيرية التي تم الحصول عليها في هذه الدراسة متوسطة، مما يشير إلى وجود متغيرات أخرى مؤثرة على مخاوف الخصوصية والتي لم يتم أخذها في الإعتبار. فى ضوء هذا القيد يمكن للباحثين بذل المزيد من الجهد من أجل دراسة تأثير متغيرات أخرى مثل العوامل الديموجرافية، السمات الشخصية، كفاءة الإنترنت، نوع الوسيلة المستخدمة للتعامل مع روبوتات الدردشة.
- في حين أن نموذج الدراسة يعتمد على الدمج بين كل من نظرية "التنمية متعددة الأبعاد" (MDT)، ونموذج "المسببات - مخاوف الخصوصية - النتائج" (APCO)، إلا أن هناك مجموعة من النظريات يمكن استخدامها فى الأبحاث المستقبلية مثل نظرية حساب الخصوصيةPrivacy Calculus Theory ، نظرية دافع الحماية Protection Motivation Theory

- قد توسع الدراسات المستقبلية من ملف المستجيبين بالإعتماد على عينة أكبر وأكثر تنوعاً بالتطبيق على خدمات أخرى على سبيل المثال، الخدمات القانونية والصحية، خدمات الضيافة والمطاعم. والتنوع أيضاً فى استخدام تطبيقات أخرى للذكاء الاصطناعى بخلاف روبوتات الدردشة مثل، استخدام تطبيقات التعرف على بيانات العميل باستخدام التعرف على الوجه، أو الصوت، مما قد يساعد في الحصول على نظرة أعمق فيما يتعلق بالسلوك الذي ينتهجه المستخدمون تجاه أدوات الذكاء الاصطناعى.
- قد ينشأ قيد آخر من حيث النطاق الجغرافي الذى تم اختياره لهذه الدراسة - البنوك فى محافظتى القاهرة والجيزة- وتشجيعاً للبحوث المستقبلية يمكن تكرار تقييم النموذج المقترح في محافظات أخرى.
- اهتمت الدراسة بالنتائج السلوكية المترتبة على مخاوف الخصوصية مثل التجنب السلوكى والإفصاح عن المعلومات، قد تهتم الدراسات المستقبلية بنتائج سلوكية أخرى مثل النية للشراء، الكلمة المنطوقة، المشاركة الاجتماعية، والمشاركة فى الأنشطة الترويجية.
- تم استخدم الدراسة المقطعية Cross Sectional، مما يجعل من الصعب تحديد العلاقات السببية بين المتغيرات، يمكن للأبحاث اللاحقة أن تستخدم الدراسات الطولية لفهم الأنماط المتغيرة للمعرفة حول مخاوف الخصوصية والنتائج السلوكية المترتبة عليها، واختبار تأثيرات هذه المتغيرات بدقة مع مرور الوقت.

المراجع

أولاً: المراجع باللغة العربية

الهيئة العامة للاستعلامات.(4 يوليو،2023) القطاع المصرفى.

https://indicator of economic strength and resilience.Where we can and how we have become - the State Information Service

عبد الرحمن، دعاء حامد محمد (2022). الموافقة ودورها في تقنين التعامل في البيانات الصحية الحساسة وتأثيرها على الأمن المعلوماتي قراءة في قانون حماية البيانات الشخصية رقم 151 لسنة 2020. **مجلة الدراسات القانونية والاقتصادية**،8، 49–1.

علي،علياء علي زكريا(2023). حماية البيانات الشخصية الطبية الحساسة وفق منظور تطور حماية الحق في الصحة (دراسة مقارنة). **مجلة روح القوانين**،104(1)،111–342.

رجب، ياسر محمد عبد السلام (2022). التطورات التشريعية المستحدثة في مجال الأمن المعلوماتي– دراسة مقارنة. **المجلة العربية للمعلوماتية وأمن المعلومات**، 3(6)، 115–152.

ثانياً: المراجع باللغة الأجنبية

Abdulquadri, A., Mogaji, E., Kieu, T. A., & Nguyen, N. P. (2021). Digital transformation in financial services provision: A Nigerian perspective to the adoption of chatbot. *Journal of Enterprising Communities: People and Places in the Global Economy*, *15*(2), 258-281.

Abdulrahman, D. H. M. (2022). Consent and its role in regulating the handling of sensitive health data and its impact on information security: A reading in Personal Data Protection Law No.151 of 2020. *Journal of Legal and Economic Studies*, 8, 1-49. (In Arabic)

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347(6221), 509–514.

Adam, M., Wessel, M., & Benlian, A. (2021). AI-based chatbots in customer service and their effects on user compliance. *Electronic Markets*, 31(2), 427-445.

Adamopoulou, E., & Moussiades, L. (2020). Chatbots: History, technology, and applications. *Machine Learning with applications*, *2*, 100006.

Adhikari, K., & Panda, R. K. (2018). Users' information privacy concerns and privacy protection behaviors in social networks. *Journal of Global Marketing*, 31(2), 96-111.

Aiolfi, S., Bellini, S., & Pellegrini, D. (2021). Data-driven digital advertising: Benefits and risks of online behavioral advertising. *International Journal of Retail and Distribution Management*, 49(7), 1089–1110.

Aivazpour, Z., & Rao, V. S. (2019). Impulsivity and information disclosure: Implications for privacy paradox. In *Proceedings of the 52nd Hawaii International Conference on System Sciences,*4861-4874.

Alashoor, T., Han, S., & Joseph, R. C. (2017). Familiarity with big data, privacy concerns, & self-disclosure accuracy in social networking websites: An APCO model. *Communications of the Association for Information Systems*, 41(1), 96-110.

Aly,A.Z.(2023).Protection of sensitive medical personal data from the perspective of the development of the right to health protection (Comparative study). *Journal of the Spirit of Laws*, 104(1), 111-342. (in Arabic)

Al-Jabri, I. M., Eid, M. I., & Abed, A. (2019). The willingness to disclose personal information: Trade-off between privacy concerns and benefits. *Information & Computer Security*, *28*(2), 161-181.

Anic, I. D., Budak, J., Rajh, E., Recher, V., Skare, V., & Skrinjaric, B. (2019). Extended model of online privacy concern: what drives consumers' decisions?. *Online Information Review*, *43*(5), 799-817.

Ashfaq, M., Yun, J., Yu, S., & Loureiro, S. M. C. (2020). I, chatbot: Modeling the determinants of users' satisfaction and continuance intention of AI-powered service agents. *Telematics and Informatics*, 54, 101473.

Aslam, U. (2023). Understanding the usability of retail fashion brand chatbots: Evidence from customer expectations and experiences. *Journal of Retailing and Consumer Services*, *74*, 103377.

Baklouti, F., & Boukamcha, F. (2023). Consumer resistance to internet banking services: Implications for the innovation resistance theory. *Journal of Financial Services Marketing*, 1-13.

Bandara, R., Fernando, M., & Akter, S. (2021). Managing consumer privacy concerns and defensive behaviours in the digital marketplace. *European Journal of Marketing*, *55*(1), 219-246.

Bano, S., Mirza, M. Z., Sohail, M., & Javaid, M. U. (2022). Privacy matters: Impact of ethical organization care & government regulations on customer patronage. *EuroMed Journal of Business*.

Bartol, J., Prevodnik, K., Vehovar, V., & Petrovčič, A. (2022). The roles of perceived privacy control, Internet privacy concerns, & Internet skills in the direct & indirect Internet uses of older adults: Conceptual integration & empirical testing of a theoretical model. *New Media & Society*,1-21.

Bartol, J., Vehovar, V., Bosnjak, M., & Petrovčič, A. (2023). Privacy concerns and self-efficacy in e-commerce: Testing an extended APCO model in a prototypical EU country. *Electronic Commerce Research and Applications*, 60, 101289.

Baumeister, R. F., & Leary, M. R. (2017). The need to belong: Desire for interpersonal attachments as a fundamental human motivation . *Interpersonal development*, 57-89.

Bekmanis, N. (2023). *Artificial Intelligence Conversational Agents: A Measure of Satisfaction in Use.* (Unpublished Master's dissertation), University of Twente, Netherlands.

Benamati, J. H., Ozdemir, Z. D., & Smith, H. J. (2016). An empirical test of an Antecedents–Privacy Concerns–Outcomes model. *Journal of Information Science*, *43*(5), 583-600.

Biswas, S., Carson, B., Chung, V., Singh, S., & Thomas, R. (2020). *AI-bank of the future: Can banks meet the AI challenge*. New York, NY: McKinsey & Company.

Bleier, A., Goldfarb, A., & Tucker, C. (2020). Consumer privacy and the future of data-based innovation and marketing. *International Journal of Research in Marketing*, *37*(3), 466-480.

Blut, M., Wang, C., Wünderlich, N. V., & Brock, C. (2021). Understanding anthropomorphism in service provision: a meta-analysis of physical robots, chatbots, and other AI. *Journal of the Academy of Marketing Science*, *49*, 632-658.

Boerman, S. C., Kruikemeier, S., & Bol, N. (2021). When is personalized advertising crossing personal boundaries? How type of information, data sharing, and personalized pricing influence consumer perceptions of personalized advertising. *Computers in Human Behavior Reports*, *4*, 100144.

Boggavarapu, S. (2021). *The Effect of Third-Party Service Providers on Information Security Breaches at Financial Institutions.* (Unpublished Doctoral dissertation), University of the Cumberlands, United States.

Bouhia, M., Rajaobelina, L., PromTep, S., Arcand, M., & Ricard, L. (2022). Drivers of privacy concerns when interacting with a chatbot in a customer service encounter. *International Journal of Bank Marketing*, *40*(6), 1159-1181.

Cao, X., & Yu, L. (2019). Exploring the influence of excessive social media use at work: A three-dimension usage perspective. *International Journal of Information Management*, *46*, 83-92.

Carmeli, A., Brammer, S., Gomes, E., & Tarba, S. Y. (2017). An organizational ethic of care and employee involvement in sustainability-related behaviors: A social identity perspective. *Journal of Organizational Behavior*, *38*(9), 1380-1395.

Chen, H. L., Widarso, G., & Sutrisno, H. (2020). A chatbot for learning Chinese: Learning achievement and technology acceptance. *Journal of Educational Computing Research*, *58*(6), 1161-1189.

Cheng, X., Qiao, L., Yang, B., & Zhang, X. (2022). Investigation on users' resistance intention to facial recognition payment: a perspective of privacy. *Electronic Commerce Research*, 1-27.

Cho, C. H., & Cheon, H. J. (2004). Why do people avoid advertising on the internet?. *Journal of advertising*, 33(4), 89-97.

Chong, T., Yu, T., Keeling, D. I., & de Ruyter, K. (2021). AI-chatbots on the services frontline addressing the challenges and opportunities of agency. *Journal of Retailing and Consumer Services*, *63*, 102735.

Choudhury, A., & Shamszare, H. (2023). Investigating the impact of user trust on the adoption and use of ChatGPT: Survey analysis. *Journal of Medical Internet Research*, *25*, e47184.

Chung, M., Ko, E., Joung, H., & Kim, S. J. (2020). Chatbot e-service and customer satisfaction regarding luxury brands. *Journal of Business Research*, *117*, 587-595.

Coskun, M., Saygili, E., & Karahan, M. O. (2022). Exploring online payment system adoption factors in the age of COVID-19—Evidence from the Turkish banking industry. *International Journal of Financial Studies*, *10*(2), 39.

Cottrill, C. D., Jacobs, N., Markovic, M., & Edwards, P. (2020). Sensing the city: designing for privacy and trust in the internet of things. *Sustainable Cities and Society*, *63*, 102453.

Creswell, J. W., & Plano Clark, V. L. (2017). *Designing and conducting mixed methods research* (3rd ed.). Sage publications.

Dabholkar, P. A., & Bagozzi, R. P. (2002). An attitudinal model of technology-based self-service: moderating effects of consumer traits and situational factors. *Journal of the academy of marketing science*, *30*, 184-201.

Davenport, T., Guha, A., Grewal, D., & Bressgott, T. (2020). How artificial intelligence will change the future of marketing. *Journal of the Academy of Marketing Science*, *48*, 24-42.

Degirmenci, K. (2020). Mobile users' information privacy concerns and the role of app permission requests. *International Journal of Information Management*, *50*, 261-272.

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, *22*(3), 295-316.

Dodoo, N. A., & Wen, J. (2019). A path to mitigating SNS ad avoidance: Tailoring messages to individual personality traits. *Journal of Interactive Advertising*, *19*(2), 116-132.

Dogra, N., Adil, M., Sadiq, M., Rafiq, F., & Paul, J. (2022). Demystifying tourists' intention to purchase travel online: the moderating role of technical anxiety and attitude. *Current Issues in Tourism*, *26*(13), 2164-2183.

Duong, C. D., Ngo, T. V. N., Khuc, T. A., Tran, N. M., & Nguyen, T. P. T. (2024). Unraveling the dark side of ChatGPT: a moderated mediation model of technology anxiety and technostress. *Information Technology & People*.

Eren, B. A. (2021). Determinants of customer satisfaction in chatbot use: evidence from a banking application in Turkey. *International Journal of Bank Marketing*, *39*(2), 294-311.

European Union Agency for Cybersecurity. (2023, November 21). Data Protection: Privacy enhancing technologies. https://www.enisa.europa.eu/topics/data-protection/privacy-enhancing-technologies

Fan, A., Lu, Z., & Mao, Z. E. (2022). To talk or to touch: Unraveling consumer responses to two types of hotel in-room technology. *International Journal of Hospitality Management*, *101*, 103112.

Følstad, A., Nordheim, C. B., & Bjørkli, C. A. (2018). What makes users trust a chatbot for customer service? An exploratory interview study. *In Internet Science: 5th International Conference, Russia, 24–26.*

Fornell, *C., & Larcker, D.F. (1981). Structural equation models with unobservable variables and measurement error: algebra and statistics. Journal of Marketing Research, 18, 382–388.*

Gefen, D. (2000). E-commerce: the role of familiarity and trust. *Omega*, *28*(6), 725-737.

Ginosar, A., & Ariel, Y. (2017). An analytical framework for online privacy research: What is missing?. *Information & Management*, *54*(7), 948-957.

Gouthier, M. H., Nennstiel, C., Kern, N., & Wendel, L. (2022). The more the better? Data disclosure between the conflicting priorities of privacy concerns, information sensitivity and personalization in e-commerce . *Journal of Business Research*, *148*, 174-189.

Griffin, A. C., Xing, Z., Mikles, S. P., Bailey, S., Khairat, S., Arguello, J., & Chung, A. E. (2021). Information needs and perceptions of chatbots for hypertension medication self-management: a mixed methods study . *JAMIA open*, *4*(2), 1-10.

Guest, G., Namey, E. E., & Mitchell, M. L. (2013). *Collecting qualitative data: A field manual for applied research*. London: Sage Publications.

Guo, Y., Lu, Z., Kuang, H., & Wang, C. (2020). Information avoidance behavior on social network sites: Information irrelevance, overload, and the moderating role of time pressure. *International Journal of Information Management*, *52*, 102067.

Ha, Q. A., Chen, J. V., Uy, H. U., & Capistrano, E. P. (2021). Exploring the privacy concerns in using intelligent virtual assistants under perspectives of information sensitivity and anthropomorphism. *International journal of human–computer interaction*, *37*(6), 512-527.

Haenlein, M., Huang, M. H., & Kaplan, A. (2022). Guest editorial: Business ethics in the era of artificial intelligence. *Journal of Business Ethics*, *178*(4), 867-869.

Ham, C. D. (2017). Exploring how consumers cope with online behavioral advertising. *International Journal of Advertising*, *36*(4), 632-658.

Hair Jr, J. F., Hult, G. T. M., Ringle, C. M., Sarstedt, M., Danks, N. P., & Ray, S. (2021). *Partial least squares structural equation modeling (PLS-SEM) using R*. Cham, Switzerland: Springer Nature Switzerland.

Hair Jr, J., Page, M., & Brunsveld, N. (2019). *Essentials of business research methods*. Routledge.

Hair, J., Hult, G., Ringle, C., & Sarstedt, M. (2014). *A primer on partial least squares structural equation modelling (PLS-SEM).* Sage Publications, Los Angeles.

Hair Jr, J., Black, W., Babin, B., & Anderson, R. (2010). *Multivariate data analysis* (7th ed.). Pearson Prentice Hall, New York.

Harborth, D., & Pape, S. (2021). Investigating privacy concerns related to mobile augmented reality Apps–A vignette based online experiment . *Computers in Human Behavior*, *122*, 106833.

Hariri, W. (2023). Unlocking the potential of ChatGPT: A comprehensive exploration of its applications, advantages, limitations, and future

directions in natural language processing. *arXiv preprint arXiv:2304. 02017*.

Henderson, K. (2011). Post-positivism and the pragmatics of leisure research. *Leisure Sciences, 33*(4), 341–346.

Hong, W., Chan, F. K., & Thong, J. Y. (2021). Drivers and inhibitors of internet privacy concern: a multidimensional development theory perspective . . *Journal of Business Ethics, 168*(3), 539-564.

Houghton, J. D., Pearce, C. L., Manz, C. C., Courtright, S., & Stewart, G. L. (2015). Sharing is caring: Toward a model of proactive caring through shared leadership. *Human resource Management review*, *25*(3), 313-327.

Hsu, C. L., & Lin, J. C. C. (2023). Understanding the user satisfaction and loyalty of customer service chatbots. *Journal of Retailing and Consumer Services*, *71*, 103211.

Hu, Y., & Min, H. K. (2023). The dark side of artificial intelligence in service: The "watching-eye" effect and privacy concerns. *International Journal of Hospitality Management*, *110*, 103437.

Immonen, M., Sintonen, S., & Koivuniemi, J. (2018). The value of human interaction in service channels. *Computers in Human Behavior*, *78*, 316-325.

Inan, D. I., Hidayanto, A. N., Juita, R., Andiyani, K., Hariyana, N., Tiffany, P., & Kurnia, S. (2022). Technology anxiety and social influence towards intention to use of ride-hailing service in Indonesia. *Case Studies on Transport Policy*, *10*(3), 1591-1601.

Ioannou, A., Tussyadiah, I., & Lu, Y. (2020). Privacy concerns and disclosure of biometric and behavioral data for travel. *International Journal of Information Management*, *54*, 102122.

Ischen, C., Araujo, T., Voorveld, H., Van, G., & Smit, E. (2020). Privacy concerns in chatbot interactions. In *Chatbot Research and Design: Third International Workshop, Conversations 2019, Amsterdam, The Netherlands, 19–20.*

Ivanov, S. H., & Umbrello, S. (2021). The ethics of artificial intelligence and robotisation in tourism and hospitality–a conceptual framework and research agenda. *Journal of Smart Tourism*, *1*(4), 9-18.

Jain, S., & Purohit, H. C. (2022). Privacy concerns and avoidance behaviour towards data-driven online behavioural advertising. *Business Analyst Journal*, *43*(1), 1-12.

Jang, M., Jung, Y., & Kim, S. (2021). Investigating managers' understanding of chatbots in the Korean financial industry. *Computers in Human Behavior*, *120*, 106747.

Jayasuriya, N. A., Udadeniya, U. P. R. P., & Yalegama, M. M. H. H. (2021). Behavioural advertising avoidance in online retail industry. *International Journal of Scientific & Technology Research*, 10(4), 15-23.

Jha, S., Gupta, S., & Mahajan, R. (2023). The effect of motivated consumer innovativeness on the intention to use chatbots in the travel and tourism sector. *Asia Pacific Journal of Tourism Research*, *28*(7), 729-744.

Jozani, M., Ayaburi, E., Ko, M., & Choo, K. K. R. (2020). Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective. *Computers in Human Behavior*, *107*, 106260.

Kamal, S. A., Shafiq, M., & Kakria, P. (2020). Investigating acceptance of telemedicine services through an extended technology acceptance model (TAM). *Technology in Society*, *60*, 101212.

Kelly, L., Kerr, G., & Drennan, J. (2020). Triggers of engagement and avoidance: Applying approach-avoid theory. *Journal of marketing communications* , *26*(5), 488-508.

Khan (2024). Survey on Online Privacy Concerns Using LinkedIn and Its Impact on Consumer Behaviour: A Study in Kalyani, Bengal. *Contemporary Is Accounting*, 157-161.

Khoury, R., Avila, A. R., Brunelle, J., & Camara, B. M. (2023, October). How secure is code generated by ChatGPT?. In *2023 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, 2445-2451.

Kim, M., Oh, J., & Kim, B. (2021). Experience of digital music services and digital self-efficacy among older adults: Enjoyment and anxiety as mediators. *Technology in society*, *67*, 101773.

Kolotylo-Kulkarni, M., Xia, W., & Dhillon, G. (2021). Information disclosure in e-commerce: A systematic review and agenda for future research. *Journal of Business Research*, *126*, 221-238.

Kowalewski, S., Ziefle, M., Ziegeldorf, H., & Wehrle, K. (2015). Like us on Facebook!–Analyzing user preferences regarding privacy settings in Germany. *Procedia Manufacturing*, *3*, 815-822.

Kroll, T., & Stieglitz, S. (2021). Digital nudging and privacy: improving decisions about self-disclosure in social networks. *Behaviour & Information Technology*, *40*(1), 1-19.

Kruikemeier, S., Boerman, S. C., & Bol, N. (2020). Breaching the contract? Using social contract theory to explain individuals' online behavior to safeguard privacy. *Media Psychology*, *23*(2), 269-292.

Landim, A., Pereira, A., Vieira, T., Costa, E., Moura, J., Wanick, V., & Bazaki, E. (2022). Chatbot design approaches for fashion e-commerce: An interdisciplinary review. *International Journal of Fashion Design, Technology and Education*, 15(2), 200-210.

Lang, M., Wiesche, M., & Krcmar, H. (2018). Perceived control & privacy in a professional cloud environment. In *Proceedings of the 51st Hawaii International Conference on System Sciences*, 3668-3677.

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of social Issues*, *33*(3), 22-42.

Le, C., Zhang, Z., & Liu, Y. (2024). Research on Privacy Disclosure Behavior of Mobile App Users from Perspectives of Online Social Support and Gender Differences. *International Journal of Human–Computer Interaction*, 1-15.

Lee, H. J. (2017). Personality determinants of need for interaction with a retail employee and its impact on self-service technology (SST) usage intentions. *Journal of Research in Interactive Marketing*, *11*(3), 214-231.

Lee, K. Y., Sheehan, L., Lee, K., & Chang, Y. (2021). The continuation and recommendation intention of artificial intelligence-based voice assistant systems (AIVAS): the influence of personal traits. *Internet Research, 31*(5), 1899-1939.

Lee, S., Ha, H. R., Oh, J. H., & Park, N. (2018). The impact of perceived privacy benefit and risk on consumers' desire to use internet of things technology. In *Human Interface and the Management of Information. Information in Applications and Services: 20th International Conference*, 609-619.

Li, Y. (2014). The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns. *Decision support systems*, *57*, 343-354.

Limakrisna, N., & Moeins, A. (2024). Intelligent Banking Chatbot: Intention to Continue Through Millennial Customer Satisfaction in Indonesia Using the TAM Method. *Dinasti International Journal of Economics, Finance & Accounting (DIJEFA)*, *4*(6).

Ling, E. C., Tussyadiah, I., Tuomi, A., Stienmetz, J., & Ioannou, A. (2021). Factors influencing users' adoption and use of conversational agents: A systematic review. *Psychology & marketing*, *38*(7), 1031-1051.

Liu, Y. L., Hu, B., Yan, W., & Lin, Z. (2023). Can chatbots satisfy me? A mixed-method comparative study of satisfaction with task-oriented chatbots in mainland China and Hong Kong. *Computers in Human Behavior*, 143, 107716.

Liu, Y. L., Yan, W., & Hu, B. (2021). Resistance to facial recognition payment in China: The influence of privacy-related factors. *Telecommunications Policy*, *45*(5), 102155.

Luo, B., Lau, R., Li, C., & Si, Y. (2022). A critical review of state-of-the-art chatbot designs and applications. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 12(1), e1434.

Lutz, C., & Newlands, G. (2021). Privacy and smart speakers: A multi-dimensional approach. *The Information Society*, 1–16.

Maduku, D. K., Mpinganjira, M., Rana, N. P., Thusi, P., Ledikwe, A., & Mkhize, N. H. B. (2023). Assessing customer passion, commitment, and word-of-mouth intentions in digital assistant usage: the moderating role of technology anxiety. *Journal of Retailing and Consumer Services*, *71*, 103208.

Malodia, S., Kaur, P., Ractham, P., Sakashita, M., & Dhir, A. (2022). Why do people avoid and postpone the use of voice assistants for transactional purposes? A perspective from decision avoidance theory. *Journal of Business Research*, *146*, 605-618.

Markets & Markets. (2024, March 18). Chatbot Market. https://www.marketsandmarkets.com/Market-Reports/chatbot-market- 72302363.html

Mattison Thompson, F., & Siamagka, N. T. (2022). Counteracting consumer subversion: Organizational privacy ethical care as driver of online information sharing. *Psychology & Marketing*, *39*(3), 579-597.

Melumad, S., & Meyer, R. (2020). Full disclosure: How smartphones enhance consumer self-disclosure. *Journal of Marketing*, *84*(3), 28-45.

Meng, F., Guo, X., Peng, Z., Ye, Q., & Lai, K. H. (2022). Trust and elderly users' continuance intention regarding mobile health services: the contingent role of health and technology anxieties. *Information Technology & People*, *35*(1), 259-280.

Meyer-Waarden, L., Pavone, G., Poocharoentou, T., Prayatsup, P., Ratinaud, M., Tison, A., & Torné, S. (2020). How service quality influences customer acceptance and usage of chatbots?. *SMR-Journal of Service Management Research*, *4*(1), 35-51.

Mimoun, M. S. B., Poncin, I., & Garnier, M. (2017). Animated conversational agents and e-consumer productivity: The roles of agents and individual characteristics. *Information & Management*, *54*(5), 545-559.

Mogaji, E., & Nguyen, N. P. (2022). Managers' understanding of artificial intelligence in relation to marketing financial services: insights from a cross-country study. *International Journal of Bank Marketing*, *40*(6), 1272-1298.

Mogaji, E., Balakrishnan, J., Nwoba, A. C., & Nguyen, N. P. (2021). Emerging-market consumers' interactions with banking chatbots. *Telematics and Informatics*, *65*, 101711.

Morimoto, M. (2020). Privacy concerns about personalized advertising across multiple social media platforms in Japan: The relationship with information control and persuasion knowledge. *International Journal of Advertising*, 1–21.

Mozafari, N., Weiger, W. H., & Hammerschmidt, M. (2022). Trust me, I'm a bot–repercussions of chatbot disclosure in different service frontline settings. *Journal of Service Management*, *33*(2), 221-245.

Mutimukwe, C., Kolkowska, E., & Grönlund, Å. (2020). Information privacy in e-service: Effect of organizational privacy assurances on individual privacy concerns, perceptions, trust and self-disclosure behavior. *Government Information Quarterly*, *37*(1), 101413.

National Institute of Standards and Technology. (2024, January 20). Privacy Engineering Objectives and Risk Model Discussion Draft. https://www.nist.gov/system/files/documents/itl/csd/nist_privacy_engr_objectives_risk_model_discussion_draft.pdf

Neto, N. N., Madnick, S., de Paula, A. M. G., & Malara Borges, N. (2021). A case study of the Capital One data breach: Why didn't compliance requirements help prevent it?. *Journal of Information System Security*, 17(1).

Ng, M., Coopamootoo, K. P., Toreini, E., Aitken, M., Elliot, K., & Van, A. (2020). Simulating the effects of social presence on trust, privacy concerns & usage intentions in automated bots for finance. In *2020 IEEE European Symposium on Security and Privacy Workshops.*190-199.

Ngai, E. W., Lee, M. C., Luo, M., Chan, P. S., & Liang, T. (2021). An intelligent knowledge-based chatbot for customer service. *Electronic Commerce Research and Applications*, *50*, 101098.

Ni, S. (2023). How do privacy concerns affect consumers' self-disclosure on social media? In *2023 7th International Seminar on Education, Management and Social Sciences.* 953-962.

Nicholson, J., & Kurucz, E. (2019). Relational leadership for sustainability: Building an ethical framework from the moral theory of 'ethics of care'. *Journal of Business Ethics, 156,* 25-43.

Nißen, M., Selimi, D., Janssen, A., Cardona, D. R., Breitner, M. H., Kowatsch, T., & von Wangenheim, F. (2022). See you soon again, chatbot? A design taxonomy to characterize user-chatbot relationships with different time horizons. *Computers in Human Behavior, 127*, 107043.

Olt, C., & Wagner, A. (2020). Having two conflicting goals in mind: The tension between IS security and privacy when avoiding threats. In *Proceedings of the 53rd Hawaii International Conference on System Sciences.* 4213-4222.

Osatuyi, B. (2015). Is lurking an anxiety-masking strategy on social media sites? The effects of lurking and computer anxiety on explaining information privacy concern on social media platforms. *Computers in Human Behavior, 49*, 324-332.

Ozdemir, Z. D., Smith, H. J., & Benamati, J. H. (2018). Antecedents and outcomes of information privacy concerns in a peer context: An exploratory study. *European Journal of Information Systems,* 26(6), 642–660.

Pallant, J., & Manual, S. S. (2016). *A step by step guide to data analysis using IBM SPSS* (6th ed.). USA: McGraw-Hill Education.

Park, Y. J. (2021). *The future of digital surveillance: Why digital monitoring will never lose its appeal in a world of algorithm-driven AI*. University of Michigan Press.

Paul, M., Maglaras, L., Ferrag, M. A., & Almomani, I. (2023). Digitization of healthcare sector: A study on privacy and security concerns. *ICT Express*, *9*(4), 571-588.

Pickard, A. J. (2013). *Research methods in information*. Facet Publishing.

Pinochet, L. H. C., de Gois, F. S., Pardim, V. I., & Onusic, L. M. (2024). Experimental study on the effect of adopting humanized and non-humanized chatbots on the factors measure the intensity of the user's perceived trust in the Yellow September campaign. *Technological Forecasting and Social Change*, *204*, 123414.

Ragab, Y. M. A. (2022). Emerging Legislative Developments in the Field of Information Security - A Comparative Study. *Arab Journal of Informatics and Information Security*, 3(6), 121.(in Arabic)

Rajaobelina, L., Prom Tep, S., Arcand, M., & Ricard, L. (2021). Creepiness: Its antecedents and impact on loyalty when interacting with a chatbot. *Psychology & Marketing*, *38*(12), 2339-2356.

Rani, R., Kanda, J., Chanchal, C., & Vij, T. S. (2023). A Study on Chatbots in the Indian Banking Sector. In *Contemporary Studies of Risks in Emerging Technology*. 35-47.

Rath, D. K., & Kumar, A. (2021). Information privacy concern at individual, group, organization and societal level-a literature review. *Vilakshan-XIMB Journal of Management*, *18*(2), 171-186.

Rese, A., Ganster, L., & Baier, D. (2020). Chatbots in retailers' customer communication: How to measure their acceptance?. *Journal of Retailing and Consumer Services*, *56*, 102176.

Riedel, A., Mulcahy, R., & Northey, G. (2022). Feeling the love? How consumer's political ideology shapes responses to AI financial service delivery. *International Journal of Bank Marketing*, *40*(6), 1102-1132.

Rodríguez-Priego, N., Porcu, L., Pena, M. B. P., & Almendros, E. C. (2023). Perceived customer care and privacy protection behavior: The mediating role of trust in self-disclosure. *Journal of Retailing and Consumer Services*, *72*, 103284.

Roozen, I., Raedts, M., & Waetermans, G. (2022). Does a chatbot's location influence consumer attitude and intentions?. *International Journal of Internet Marketing and Advertising*.1-18.

Rudolph, J., Ismail, M. F. B. M., & Popenici, S. (2024). Higher education's generative artificial intelligence paradox: The meaning of chatbot mania. *Journal of University Teaching and Learning Practice*, *21*(6), 1-35.

Satheesh, M. K., Samala, N., & Rodriguez, R. V. (2020). Role of Ai-induced chatbot in enhancing customer relationship management in the banking industry. *ICTACT Journal on Management Studies*, *6*(4), 1320-1323.

Sanny, L., Susastra, A., Roberts, C., & Yusramdaleni, R. (2020). The analysis of customer satisfaction factors which influence chatbot acceptance in Indonesia. *Management Science Letters*, *10*(6), 1225-1232.

Sarbabidya, S., & Saha, T. (2020). Role of chatbot in customer service: A study from the perspectives of the banking industry of Bangladesh. *International review of business research papers*, *16*(1), 231-248.

Sarstedt, M., Hair Jr, J. F., & Ringle, C. M. (2023). PLS-SEM: indeed a silver bullet –retrospective observations and recent advances. *Journal of Marketing Theory and Practice*, *31*(3), 261-275.

Shannon-Baker, P. (2016). Making paradigms meaningful in mixed methods research. *Journal of mixed methods research*, *10*(4), 319-334.

Schmidt, L., Bornschein, R., & Maier, E. (2020). The effect of privacy choice in cookie notices on consumers' perceived fairness of frequent price changes. *Psychology & Marketing*, *37*(9), 1263-1276.

Schomakers, E. M., Lidynia, C., Müllmann, D., & Ziefle, M. (2019). Internet users' perceptions of information sensitivity–insights from Germany . *International Journal of Information Management*, *46*, 142-150.

Sebastian, G. (2023). Privacy and data protection in chatgpt and other ai chatbots: Strategies for securing user information. *International Journal of Security and Privacy in Pervasive Computing (IJSPPC)*, *15*(1), 1-14.

Senadheera, S., Yigitcanlar, T., Desouza, K. C., Mossberger, K., Corchado, J., Mehmood, R., & Cheong, P. H. (2024). Understanding Chatbot Adoption in Local Governments: A Review and Framework. *Journal of Urban Technology*, 1-35.

Shaeffer, T., & Keever, M. (2021). Privacy as a collective norm. *Loyola of Los Angeles Entertainment Law Review*, 41, 253–303.

Sheng, X., Felix, R., Saravade, S., Siguaw, J. A., Ketron, S. C., Krejtz, K., & Duchowski, A. T. (2020). Sight unseen: The role of online security indicators in visual attention to online privacy information. *Journal of Business Research*, *111*, 218-240.

Sidaoui, K., Jaakkola, M., & Burton, J. (2020). AI feel you: customer experience assessment via chatbot interviews. *Journal of Service Management* , 31(4), 745-766.

Singaraju, S. P., Rose, J. L., Arango-Soler, L. A., D'Souza, C., Khaksar, S. M. S., & Brouwer, A. R. (2022). The dark age of advertising: An examination of perceptual factors affecting advertising avoidance in the context of mobile youtube. *Journal of Electronic Commerce Research*, *23*(1), 13-32.

Singh, N., Sinha, N., & Liébana-Cabanillas, F. J. (2020). Determining factors in the adoption and recommendation of mobile wallet services in India: Analysis of the effect of innovativeness, stress to use and social influence. *International Journal of Information Management*, *50*, 191-205.

Škrinjarić, B., Budak, J., & Rajh, E. (2019). Perceived quality of privacy protection regulations and online privacy concern. *Economic research-Ekonomska istraživanja*, *32*(1), 982-1000.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS quarterly*, 989-1015.

Söderlund, M., Oikarinen, E. L., & Tan, T. M. (2022). The hard-working virtual agent in the service encounter boosts customer satisfaction. *The International Review of Retail, Distribution and Consumer Research*, *32*(4), 388-404.

State Information Service. (2023, July 4) banking sector (in Arabic)

https:// indicator of economic strength and resilience. Where we can and how we have become

Strebinger, A., & Treiblmaier, H. (2024). Disintermediation of consumer services through blockchain? The role of intermediary brands, value-added services, and privacy concerns. *International Journal of Information Management*, *78*, 102806.

Stubenvoll, M., Binder, A., Noetzel, S., Hirsch, M., & Matthes, J. (2024). Living is easy with eyes closed: Avoidance of targeted political advertising in response to privacy concerns, perceived personalization, and overload. *Communication Research*, *51*(2), 203-227.

Sun, Z., Zang, G., Wang, Z., Zhao, H., & Liu, W. (2023). VCAs as partners or servants? The effects of information sensitivity and anthropomorphism roles on privacy concerns. *Technological Forecasting and Social Change*, *192*, 122560.

Tao, S., Liu, Y., & Sun, C. (2024). Understanding information sensitivity perceptions and its impact on information privacy concerns in e-commerce services: Insights from China. *Computers & Security*, *138*, 103646.

The Royal Society. (2023, September 12). From Privacy to Partnership: The Role of Privacy Enhancing Technologies in Data Governance and Collaborative Analysis. https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/From-Privacy-to-Partnership.pdf

Thomaz, F., Salge, C., Karahanna, E., & Hulland, J. (2020). Learning from the Dark Web: Leveraging conversational agents in the era of hyper- privacy to enhance marketing. *Journal of the Academy of Marketing Science*, 48(1), 43–63.

Tsai, T. H., Lin, W. Y., Chang, Y. S., Chang, P. C., & Lee, M. Y. (2020). Technology anxiety and resistance to change behavioral study of a wearable cardiac warming system using an extended TAM for older adults. Public Library of Science One, *15*(1), e0227270.

Tseng, H. T., Ibrahim, F., Hajli, N., Nisar, T. M., & Shabbir, H. (2022). Effect of privacy concerns and engagement on social support behaviour in online health community platforms. *Technological Forecasting and Social Change*, *178*, 121592.

Vimalkumar, M., Sharma, S. K., Singh, J. B., & Dwivedi, Y. K. (2021). 'Okay google, what about my privacy?': User's privacy perceptions and acceptance of voice based digital assistants. *Computers in Human Behavior*, *120*, 106763.

Wang, X., & Liu, Z. (2019). Online engagement in social media: A cross-cultural comparison. *Computers in Human Behavior*, *97*, 137-150.

Wang, Y., Ahmed, S., & Bee, A. W. T. (2024). Selective avoidance as a cognitive response: examining the political use of social media and surveillance anxiety in avoidance behaviours. *Behaviour & Information Technology* , *43*(3), 590-604.

Woźniak, P. W., Karolus, J., Lang, F., Eckerth, C., Schöning, J., Rogers, Y., & Niess, J. (2021, May). Creepy technology: What is it and how do you measure it?. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 1-13.

Xie, Y., Chen, K., & Guo, X. (2020). Online anthropomorphism and consumers' privacy concern: Moderating roles of need for interaction and social exclusion. *Journal of Retailing and Consumer Services*, *55*, 102119.

Xu, H. (2007). The effects of self-construal and perceived control on privacy concerns. In *Proceedings of the 28th Annual International Conference on Information Systems (ICIS)*. Montre´al, Canada,1-14.

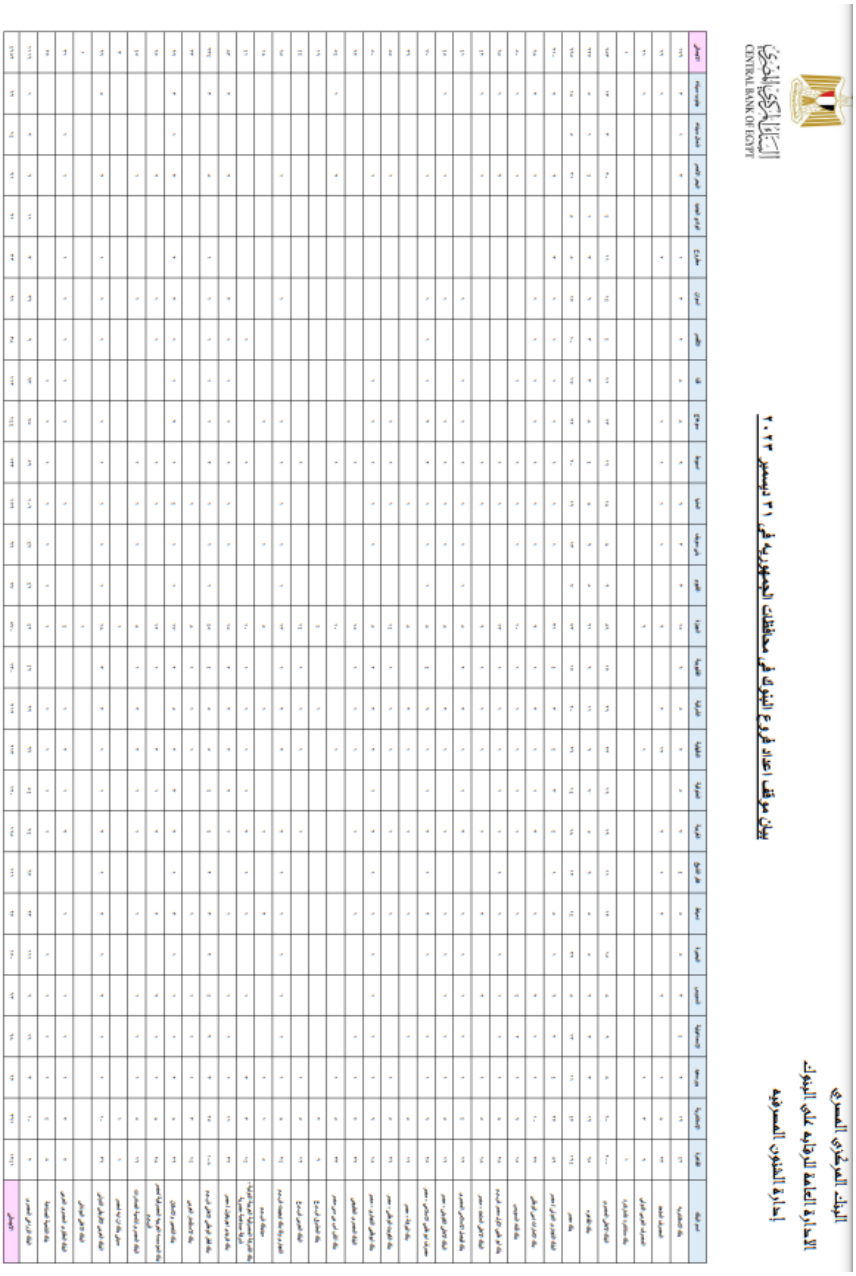
Xu, Y., Niu, N., & Zhao, Z. (2023). Dissecting the mixed effects of human-customer service chatbot interaction on customer satisfaction: An explanation from temporal and conversational cues. *Journal of Retailing and Consumer Services*, *74*, 103417.

Youn, S., & Kim, S. (2019). Understanding ad avoidance on Facebook: Antecedents and outcomes of psychological reactance. *Computers in human behavior*, *98*, 232-244.

Zhang, X., & Zhang, Z. (2024). Leaking my face via payment: Unveiling the influence of technology anxiety, vulnerabilities, and privacy concerns on user resistance to facial recognition payment. *Telecommunications Policy*, 102703.

Zhu, Y., Janssen, M., Wang, R., & Liu, Y. (2022). It is me, chatbot: working to address the COVID-19 outbreak-related mental health issues in China. User experience, satisfaction, and influencing factors. *International Journal of Human–Computer Interaction*, *38*(12), 1182-1194.

ملحق1: توزيع البنوك على المحافظات 31-12 - 2023

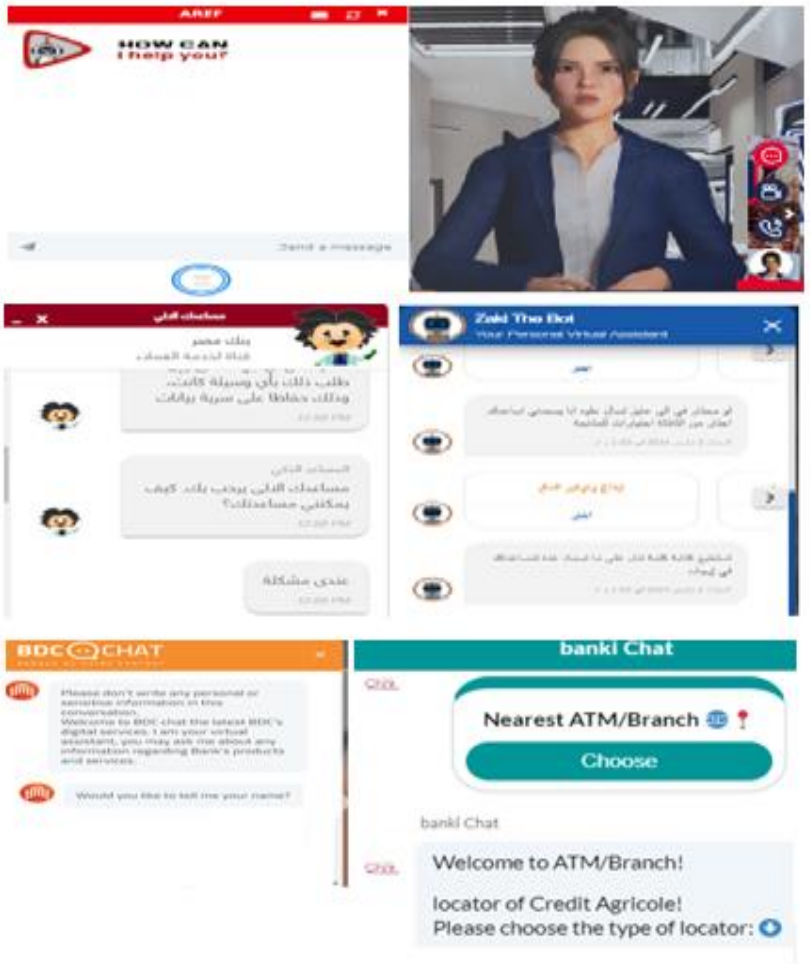

البنك المركزي المصري
الإدارة العامة للرقابة على البنوك
إدارة الفنون المصرفية

بيان بموقف اعداد فروع البنوك في محافظات الجمهورية في ٣١ ديسمبر ٢٠٢٣

البنك المركزي المصري
CENTRAL BANK OF EGYPT

ملحق 2: حساب حجم العينة باستخدام تطبيق "STATSTM 2.0"

ملحق3: صور لروبوتات الدردشة بالبنوك محل الدراسة



ملحق 4: قائمة الإستقصاء

رمزالاستجابة السريعة / QR Code

.....

Factors Influencing Privacy Concerns of Chatbot Users and their Role in Behavioural Avoidance and Information Disclosure

Dr. Nermeen Ahmed Abd Elmonem Elsaadany

Abstract

The study aims to provide a comprehensive framework for understanding the factors influencing customers' privacy concerns regarding the use of chatbots in banking service, and the impact of these concerns on behavioural avoidance and information disclosure. Data was collected using a survey distributed to a systematic sample of (365) clients from the banks operating in Egypt that offer this service. The results obtained using structural equation modelling, supported most of the study's hypotheses. Specifically, there was a positive influence of technological anxiety, familiarity with chatbot, information control, information sensitivity, government regulations and laws availability, privacy enhancing technologies, and the need for human interaction on privacy concerns. However, there was no significant effect of organizational ethical care for privacy on privacy concerns. As privacy concerns had a positive impact on behavioural avoidance and a negative impact on information disclosure.

Keywords

Technological anxiety - Familiarity with chatbot - Information control - Information sensitivity - Organizational ethical privacy care - Privacy concerns - Behavioral avoidance - Information disclosure.

التوثيق المقترح للدراسة وفقا لنظام APA

السعدني، نرمين أحمد عبد المنعم (2024). العوامل المؤثرة على مخاوف الخصوصية لمستخدمى روبوت الدردشة ودورها فى التجنب السلوكى والإفصاح عن المعلومات. **مجلة جامعة الإسكندرية للعلوم الإدارية**، 61(3)، 209-272.