

Final Project 2

PMG 497

نموذج المشروع النهائي 2

مخاطر الخصوصية المدركة وأثرها في سلوك المستخدمين في البيئة الرقمية

اسم الطالب

باسل معازر الرويلي

المشروع النهائي- 2

كلية الإدارة- جامعة ميدأوشن

إشراف

د.

عضو هيئة التدريس- كلية الإدارة- جامعة ميدأوشن

التاريخ- الفصل الدراسي

الشكر والتقدير

الحمد لله رب العالمين، والصلاة والسلام على أشرف الأنبياء والمرسلين، سيدنا محمد وعلى آله وصحبه أجمعين.

يُتقدم بخالص الشكر والتقدير إلى كل من أسهم في إنجاز هذا البحث، وقدم الدعم والتوجيه خلال مراحل إعداد، سائلاً الله أن يجزي الجميع خير الجزاء. كما يُخص بالشكر جامعة ميدأوشن وكلية الإدارة على ما قدمته من بيئة علمية ومعرفية داعمة لتطوير المهارات البحثية والأكاديمية.

كما يُتوجه بالشكر إلى المشرف الأكاديمي على ما قدمه من ملاحظات وتوجيهات كان لها أثر واضح في تحسين جودة هذا العمل، وإلى كل من قدم دعماً علمياً أو معنوياً أسهم في اكتمال هذا البحث بصورة مناسبة.

الإهداء

يُهدى هذا العمل إلى كل من كان للدعم والتشجيع أثر في مواصلة طريق العلم والبحث، وإلى كل من أسهم بكلمة أو نصيحة أو توجيه في إنجاز هذا الجهد العلمي.

كما يُهدى إلى كل من يؤمن بأهمية المعرفة، ويسعى إلى توظيف البحث العلمي في خدمة المجتمع وتطوير الممارسات الرقمية الآمنة.

ويبقى هذا العمل المتواضع ثمرة جهد علمي يُرجى أن يكون نافعاً ومفيداً للمهتمين بموضوع الخصوصية الرقمية وسلوك المستخدمين في البيئة الرقمية.

مستخلص الدراسة

الهدف: تهدف هذه الدراسة إلى تحليل مفهوم مخاطر الخصوصية المدركة في البيئة الرقمية، وبيان أثرها في اتجاهات وسلوكيات المستخدمين عند استخدام منصات التجارة الإلكترونية، وشبكات التواصل الاجتماعي، والخدمات الرقمية القائمة على جمع البيانات الشخصية.

المنهجية: اعتمدت الدراسة على المنهج الوصفي التحليلي من خلال مراجعة الأدبيات العلمية المنشورة في قواعد البيانات الأكاديمية، وبالأخص الدراسات المتاحة عبر Google Scholar، مع اقتراح تصميم ميداني كمي باستخدام استبانة تقيس إدراك المستخدمين لمخاطر الخصوصية والثقة والنية السلوكية.

النتائج: تشير الأدبيات إلى أن ارتفاع مخاطر الخصوصية المدركة يرتبط غالباً بانخفاض نية الإفصاح عن المعلومات الشخصية، وضعف الثقة في المنصات الرقمية، وتراجع نية الشراء أو الاستخدام، بينما يمكن أن تخفف عوامل مثل التحكم المدرك في المعلومات والشفافية والثقة من هذا الأثر السلبي.

التطبيقات والأهمية: تساعد نتائج الدراسة المؤسسات الرقمية على تصميم سياسات خصوصية أكثر وضوحاً، وتعزيز آليات موافقة المستخدم، وتطوير واجهات تمنح المستخدم شعوراً أعلى بالتحكم، بما يدعم الثقة والاستخدام المستدام للخدمات الرقمية.

الكلمات المفتاحية: مخاطر الخصوصية المدركة، الثقة الرقمية، الإفصاح عن المعلومات، التجارة الإلكترونية، شبكات التواصل الاجتماعي، حسابات الخصوصية.

جدول المحتويات

جدول الأشكال

جدول الجداول

1. الفصل الأول: الإطار العام للدراسة

1.1. المقدمة:

أصبحت البيانات الشخصية أحد أهم الموارد في الاقتصاد الرقمي المعاصر؛ إذ تعتمد المنصات الإلكترونية على جمعها وتحليلها لتحسين جودة الخدمات، وتخصيص تجربة المستخدم، وتوجيه الإعلانات، ودعم القرارات التسويقية والإدارية. غير أن التوسع في استخدام هذه البيانات أوجد تحديات متزايدة تتعلق بخصوصية الأفراد وأمن معلوماتهم، ولا سيما في ظل الانتشار الواسع للتجارة الإلكترونية، وشبكات التواصل الاجتماعي، وتطبيقات الذكاء الاصطناعي، وإنترنت الأشياء، التي تقوم في جوهرها على التفاعل المستمر مع بيانات المستخدمين.

وفي هذا السياق، يبرز مفهوم مخاطر الخصوصية المدركة بوصفه أحد المفاهيم المحورية لفهم سلوك المستخدم في البيئة الرقمية. ويقصد به تقدير المستخدم لاحتمال تعرض بياناته الشخصية لسوء الاستخدام، أو الوصول غير المصرح به، أو الإفصاح عنها بطرق لا يرغب فيها، وما قد يترتب على ذلك من آثار اجتماعية أو نفسية أو مالية. ولا يتشكل هذا الإدراك بناءً على مستوى الخطر الفعلي فقط، بل يتأثر أيضاً بدرجة الثقة في المنصة، ووضوح سياسات الخصوصية، وخبرة المستخدم السابقة، ومدى شعوره بالقدرة على التحكم في معلوماته الشخصية.

ومن ثم، فإن دراسة مخاطر الخصوصية المدركة لا تقتصر على الجانب التقني لحماية البيانات، بل تمتد إلى فهم العوامل النفسية والسلوكية التي تحدد مدى ثقة المستخدمين في المنصات الرقمية واستعدادهم لمشاركة معلوماتهم الشخصية أو الاستمرار في استخدام الخدمات الرقمية.

1.2. مشكلة الدراسة

تتمثل مشكلة الدراسة في أن المستخدمين يتعاملون يومياً مع منصات رقمية تطلب منهم الإفصاح عن بيانات شخصية، بينما تختلف درجة إدراكهم للمخاطر المرتبطة بهذا الإفصاح. وقد يؤدي

ارتفاع مخاطر الخصوصية المدركة إلى تقليل الثقة والحد من استخدام الخدمات الرقمية، حتى وإن كانت هذه الخدمات تقدم فوائد واضحة للمستخدم.

وبناءً على ذلك، تسعى الدراسة إلى الإجابة عن السؤال الرئيس الآتي: ما أثر مخاطر الخصوصية المدركة في سلوك المستخدمين داخل البيئة الرقمية؟ ويتفرع عن هذا السؤال بحث العلاقة بين مخاطر الخصوصية المدركة والثقة الرقمية، والنية في الإفصاح عن المعلومات، والنية في استخدام أو شراء الخدمات الرقمية.

1.2.1. فجوات على المستوى النظري

تتمثل الفجوة النظرية في الحاجة إلى مزيد من التكامل بين نماذج حسابات الخصوصية ونظرية الثقة الرقمية لفهم كيفية موازنة المستخدم بين المنافع المتوقعة من الخدمة الرقمية والمخاطر المحتملة على خصوصيته. كما أن كثيراً من الدراسات ركزت على سياقات محددة مثل التجارة الإلكترونية أو شبكات التواصل الاجتماعي، مما يبرز الحاجة إلى بناء تصور أوسع يصلح للبيئات الرقمية المتعددة.

1.2.2. فجوات على المستوى التطبيقي

تتمثل الفجوة التطبيقية في حاجة المؤسسات الرقمية إلى فهم العوامل التي تزيد أو تخفض مخاطر الخصوصية المدركة لدى المستخدمين، حتى تتمكن من تصميم سياسات وإجراءات عملية تعزز الثقة، مثل تبسيط إشعارات الخصوصية، وتوفير إعدادات تحكم واضحة، وتوضيح أغراض جمع البيانات.

1.3. أهمية الدراسة

1.3.1. على المستوى النظري:

تتبع الأهمية النظرية للدراسة من مساهمتها في إثراء الأدبيات المتعلقة بخصوصية المستخدمين في البيئة الرقمية، من خلال توضيح مفهوم مخاطر الخصوصية المدركة وربطه بمتغيرات سلوكية مهمة مثل الثقة، ونية الإفصاح عن المعلومات، ونية الاستخدام. كما تساعد الدراسة على إبراز العلاقة بين الإدراك النفسي للمخاطر والقرارات الرقمية اليومية للمستخدمين.

1.3.2. على المستوى التطبيقي:

أما الأهمية التطبيقية فتظهر في إمكانية استفادة الشركات والمنصات الرقمية وصناع القرار من نتائج الدراسة في تحسين سياسات حماية البيانات، وتقليل المخاوف المرتبطة بالخصوصية، وبناء بيئات رقمية أكثر شفافية وأماناً، الأمر الذي ينعكس إيجاباً على ثقة المستخدمين واستمرارهم في استخدام الخدمات.

1.4. أسئلة الدراسة

1. ما مستوى مخاطر الخصوصية المدركة لدى مستخدمي الخدمات الرقمية؟
2. ما أثر مخاطر الخصوصية المدركة في الثقة بالمنصات الرقمية؟
3. ما أثر مخاطر الخصوصية المدركة في نية الإفصاح عن المعلومات الشخصية؟
4. ما دور التحكم المدرك في المعلومات في تقليل مخاطر الخصوصية المدركة؟

1.5. أهداف الدراسة

1. تحديد مفهوم مخاطر الخصوصية المدركة وأبعاده الرئيسية.
2. قياس أثر مخاطر الخصوصية المدركة في الثقة الرقمية.
3. تحليل أثر مخاطر الخصوصية المدركة في نية الإفصاح عن المعلومات الشخصية.
4. اقتراح توصيات عملية للحد من مخاوف الخصوصية لدى المستخدمين.

1.6. فرضيات الدراسة

1. توجد علاقة سلبية ذات دلالة إحصائية بين مخاطر الخصوصية المدركة والثقة بالمنصات الرقمية.
2. توجد علاقة سلبية ذات دلالة إحصائية بين مخاطر الخصوصية المدركة ونية الإفصاح عن المعلومات الشخصية.
3. يسهم التحكم المدرك في المعلومات في خفض مخاطر الخصوصية المدركة.
4. تؤثر الثقة الرقمية إيجابياً في نية استخدام الخدمات الرقمية.

1.7. نموذج الدراسة

المتغير المستقل: مخاطر الخصوصية المدركة ← المتغيرات الوسيطة/المؤثرة: الثقة الرقمية والتحكم المدرك في المعلومات ← المتغيرات التابعة: نية الإفصاح عن المعلومات ونية استخدام الخدمات الرقمية.

1.8. الدراسة الميدانية

تقترح الدراسة تنفيذ جانب ميداني من خلال توزيع استبانة إلكترونية على عينة من مستخدمي الخدمات الرقمية، بهدف قياس مستوى إدراكهم لمخاطر الخصوصية وعلاقته بالثقة ونية الإفصاح عن المعلومات ونية الاستخدام. وتساعد هذه الدراسة الميدانية في تحويل الإطار النظري إلى نتائج قابلة للتحليل والمناقشة.

1.9. مخطط المشروع

يتكون مخطط المشروع من خمسة فصول رئيسية؛ يتناول الفصل الأول الإطار العام للدراسة، ويعرض الفصل الثاني الدراسات السابقة والإطار النظري، أما الفصل الثالث فيوضح منهجية الدراسة، في حين يخصص الفصل الرابع للتحليل الإحصائي ومناقشة النتائج، وينتهي البحث بالفصل الخامس الذي يعرض الحدود والتوصيات والاستنتاجات.

2. الفصل الثاني: الدراسات السابقة

2.1. المقدمة:

تناولت الدراسات السابقة موضوع الخصوصية الرقمية من زوايا متعددة، منها مخاطر الخصوصية المدركة، والتحكم في المعلومات، والثقة الرقمية، وسلوك الإفصاح عن البيانات. وتؤكد معظم الأدبيات أن قرار المستخدم في مشاركة بياناته لا يقوم على الخطر الموضوعي فقط، بل يتأثر بإدراكه الشخصي للمخاطر والمنافع المتوقعة من استخدام الخدمة.

2.2. المتغير المستقل

يمثل المتغير المستقل في هذه الدراسة «مخاطر الخصوصية المدركة»، ويقصد بها إدراك المستخدم لاحتمال تعرض بياناته الشخصية للانتهاك أو سوء الاستخدام أو الإفصاح غير المقصود. وترتبط هذه المخاطر بعوامل مثل جمع بيانات تفوق حاجة الخدمة، غموض سياسة الخصوصية، ضعف التحكم في إعدادات البيانات، وتجارب المستخدم السابقة مع تسريب أو إساءة استخدام المعلومات.

2.3. المتغير التابع

تتمثل المتغيرات التابعة في نية المستخدم للإفصاح عن معلوماته الشخصية ونية استخدامه أو استمراره في استخدام الخدمات الرقمية. فعندما يشعر المستخدم بأن المنصة لا تحمي بياناته أو لا تمنحه قدرة كافية على التحكم، قد يتجنب مشاركة معلوماته أو يقلل استخدامه للخدمة، حتى لو كانت الخدمة مفيدة أو سهلة الاستخدام.

2.4. العلاقة بين المتغير المستقل والمتغير التابع

توضح الدراسات أن العلاقة بين مخاطر الخصوصية المدركة وسلوك المستخدم غالباً ما تكون علاقة عكسية؛ فكلما زاد إدراك المستخدم للمخاطر، انخفضت ثقته ورغبته في الإفصاح والاستخدام. ومع ذلك، قد تتغير قوة هذه العلاقة بوجود عوامل وسيطة أو معدلة مثل الثقة، والمنفعة المدركة، والاهتمام الشخصي بالخدمة، والتحكم المدرك في المعلومات.

2.5. الخاتمة

يتضح من مراجعة الدراسات السابقة أن مخاطر الخصوصية المدركة تؤدي دوراً مهماً في تشكيل اتجاهات المستخدمين نحو المنصات الرقمية. فقد بينت الأدبيات أن الثقة، والتحكم المدرك في المعلومات، ووضوح سياسات الخصوصية تمثل عوامل مؤثرة في تقليل أثر هذه المخاطر على نية الإفصاح عن المعلومات ونية الاستخدام. وبذلك يوفر هذا الفصل أساساً نظرياً يدعم بناء فرضيات الدراسة واختيار منهجيتها.

3. الفصل الثالث: منهجية الدراسة

3.1. المقدمة

يعرض هذا الفصل المنهجية المقترحة لدراسة أثر مخاطر الخصوصية المدركة في سلوك المستخدمين في البيئة الرقمية. وتم اختيار المنهج الوصفي التحليلي لأنه الأنسب لفهم الظاهرة كما هي في الواقع، وتحليل العلاقات بين المتغيرات باستخدام بيانات كمية يتم جمعها من عينة من المستخدمين.

3.2. التعريفات الإجرائية لمتغيرات البحث

تعرف مخاطر الخصوصية المدركة إجرائياً بأنها الدرجة التي يعتقد فيها المستخدم أن مشاركة بياناته الشخصية مع منصة رقمية قد تؤدي إلى فقدان السيطرة على البيانات أو استخدامها دون موافقته. وتعرف الثقة الرقمية بأنها اعتقاد المستخدم بأن المنصة قادرة وراغبة في حماية بياناته. أما نية الإفصاح فهي استعداد المستخدم لتقديم معلومات شخصية عند استخدام الخدمة.

3.3. تصميم البحث والمنهج البحثي

يعتمد تصميم البحث على دراسة كمية مقطعية يتم تنفيذها من خلال استبانة إلكترونية. ويتيح هذا التصميم قياس اتجاهات المستخدمين في فترة زمنية محددة، واختبار العلاقات بين مخاطر الخصوصية المدركة والثقة ونية الإفصاح والاستخدام.

3.4. مجتمع البحث وطرق وتقنيات أخذ العينات

يتكون مجتمع البحث من مستخدمي الخدمات الرقمية مثل منصات التجارة الإلكترونية وشبكات التواصل الاجتماعي والتطبيقات الخدمية. ويمكن اختيار عينة ميسرة من المستخدمين الذين لديهم خبرة فعلية في استخدام هذه المنصات، على أن تكون العينة مناسبة للتحليل الإحصائي واختبار الفرضيات.

3.5. طريقة جمع البيانات

تجمع البيانات الأولية باستخدام استبانة تتضمن محاور تقيس مخاطر الخصوصية المدركة، والتحكم المدرك في المعلومات، والثقة الرقمية، ونية الإفصاح، ونية الاستخدام. أما البيانات الثانوية فتجمع من الدراسات العلمية والكتب والمقالات المحكمة المتاحة عبر Google Scholar وقواعد البيانات الأكاديمية ذات الصلة.

3.6. الاعتبارات الأخلاقية والموافقة المستنيرة

تلتزم الدراسة بالاعتبارات الأخلاقية اللازمة عند جمع البيانات من المشاركين، وذلك من خلال توضيح هدف الدراسة وطبيعة المشاركة قبل تعبئة الاستبانة، والتأكيد على أن المشاركة اختيارية بالكامل، وأن

للمشارك الحق في عدم الإجابة عن أي سؤال أو الانسحاب في أي وقت دون أي تبعات. كما يتم استخدام البيانات لأغراض البحث العلمي فقط، ولا تُجمع أي معلومات شخصية مباشرة يمكن أن تكشف هوية المشاركين.

وتتحقق الموافقة المستنيرة من خلال إبلاغ المشاركين بأن إجاباتهم ستعامل بسرية تامة، وأن النتائج ستعرض بصورة إجمالية دون الإشارة إلى أي فرد بعينه. ويهدف هذا الإجراء إلى حماية خصوصية المشاركين وتقليل أي مخاطر محتملة مرتبطة بالإفصاح عن آرائهم أو بياناتهم، بما ينسجم مع طبيعة موضوع الدراسة المتعلق بمخاطر الخصوصية المدركة.

3.7. أنواع البيانات

تعتمد الدراسة على نوعين من البيانات: بيانات أولية يتم الحصول عليها من إجابات أفراد العينة، وبيانات ثانوية يتم الحصول عليها من الأدبيات السابقة. وتساعد البيانات الأولية في اختبار الفرضيات، بينما توفر البيانات الثانوية أساساً نظرياً لتفسير النتائج.

3.8. إجراءات التحليل الإحصائي

تقترح الدراسة استخدام الإحصاء الوصفي لعرض خصائص العينة ومستويات المتغيرات، واختبار معامل الثبات كرونباخ ألفا للتحقق من اتساق فقرات الاستبانة، إضافة إلى تحليل الارتباط والانحدار أو نمذجة المعادلات الهيكلية لاختبار الفرضيات والعلاقات بين المتغيرات.

3.9. الخاتمة

خلص هذا الفصل إلى تحديد المنهجية المناسبة لدراسة مخاطر الخصوصية المدركة، وذلك من خلال اعتماد المنهج الوصفي التحليلي وتصميم كمي يعتمد على الاستبانة. كما أوضح الفصل مجتمع الدراسة، وطريقة جمع البيانات، وأنواع البيانات، والإجراءات الإحصائية المقترحة، بما يمهد للانتقال إلى عرض التحليل الإحصائي ومناقشة النتائج.

4. الفصل الرابع: التحليل الإحصائي ومناقشة النتائج

4.1. المقدمة

يتناول هذا الفصل عرضاً مقترحاً لآلية تحليل البيانات ومناقشة النتائج المتوقعة للدراسة. وبما أن الدراسة ذات طبيعة مقترحة، فإن هذا الفصل يوضح الأساليب التي يمكن استخدامها لتحليل إجابات أفراد العينة،

وتفسير العلاقة بين مخاطر الخصوصية المدركة والمتغيرات التابعة، بما ينسجم مع أهداف الدراسة وفرضياتها.

4.2. توصيف عينة الدراسة (الإحصائيات الوصفية لعينة البحث)

يتم توصيف عينة الدراسة من خلال عرض الخصائص الديموغرافية للمبحوثين مثل الجنس، والعمر، والمستوى التعليمي، ومدى استخدام الخدمات الرقمية. ويساعد هذا التوصيف في فهم طبيعة العينة، وتفسير الاختلافات المحتملة في إدراك مخاطر الخصوصية بين فئات المستخدمين.

4.3. اختبارات الصدق والثبات للاستبيانات

للتحقق من جودة أداة الدراسة، يمكن عرض الاستبانة على مجموعة من المحكمين للتأكد من صدق المحتوى، ثم اختبار الثبات باستخدام معامل كرونباخ ألفا. وتعد القيم المرتفعة لمعامل الثبات مؤشراً على اتساق فقرات الاستبانة وقدرتها على قياس المتغيرات بصورة مستقرة.

4.4. الإحصاء الوصفي لمتغيرات البحث (الإجابة على أسئلة البحث)

يعتمد الإحصاء الوصفي على حساب المتوسطات الحسابية والانحرافات المعيارية لفقرات الاستبانة، وذلك لتحديد مستوى مخاطر الخصوصية المدركة ومستوى الثقة الرقمية ونية الإفصاح ونية الاستخدام. وتسهم هذه المؤشرات في الإجابة عن أسئلة الدراسة وتقديم صورة عامة عن اتجاهات أفراد العينة.

4.5. اختبار الفرضيات ومناقشة النتائج

لاختبار فرضيات الدراسة، يمكن استخدام تحليل الارتباط والانحدار لقياس قوة واتجاه العلاقة بين مخاطر الخصوصية المدركة والثقة الرقمية ونية الإفصاح ونية الاستخدام. ومن المتوقع أن تظهر النتائج علاقة سلبية بين مخاطر الخصوصية المدركة والثقة ونية الإفصاح، بينما تسهم الثقة والتحكم المدرك في المعلومات في تخفيف الأثر السلبي لهذه المخاطر.

4.6. الخاتمة

يؤكد هذا الفصل أهمية التحليل الإحصائي في تحويل البيانات الميدانية إلى نتائج علمية يمكن تفسيرها وربطها بالإطار النظري. ومن خلال توصيف العينة، واختبار الصدق والثبات، وتحليل المتغيرات، واختبار الفرضيات، يمكن الوصول إلى فهم أوضح لأثر مخاطر الخصوصية المدركة في سلوك المستخدمين في البيئة الرقمية.

5. الفصل الخامس: حدود البحث والتوصيات والاستنتاجات

5.1. حدود الدراسة والدراسات المستقبلية:

تتمثل حدود الدراسة في اعتمادها على عينة من مستخدمي الخدمات الرقمية، مما قد يحد من إمكانية تعميم النتائج على جميع الفئات أو الدول. كما أن استخدام الاستبانة قد يتأثر بإدراك المبحوثين الذاتي ورغبتهم في تقديم إجابات اجتماعية مقبولة. وتقتصر الدراسة المستقبلية توسيع العينة، والمقارنة بين أنواع مختلفة من المنصات الرقمية، واستخدام أساليب نوعية مثل المقابلات لفهم أعمق لتجارب المستخدمين.

5.2. توصيات الدراسة:

1. تبسيط سياسات الخصوصية وصياغتها بلغة واضحة يفهمها المستخدم غير المتخصص.
2. توفير خيارات تحكم فعالة تمكن المستخدم من تعديل إعدادات جمع البيانات ومشاركتها.
3. تعزيز الشفافية حول أغراض جمع البيانات ومدة الاحتفاظ بها والجهات التي قد تشارك معها.
4. رفع وعي المستخدمين بممارسات حماية الخصوصية الرقمية وطرق تقليل المخاطر.

5.3. الخاتمة:

خلصت الدراسة إلى أن مخاطر الخصوصية المدركة تمثل عاملاً محورياً في تفسير سلوك المستخدمين داخل البيئة الرقمية، فهي تؤثر في الثقة، وفي استعداد المستخدمين للإفصاح عن بياناتهم الشخصية، وفي نيتهم لاستخدام الخدمات الرقمية. كما أظهرت الأدبيات أن تقليل هذه المخاطر لا يعتمد فقط على الحماية التقنية، بل يتطلب أيضاً شفافية مؤسسية، وسياسات واضحة، وتمكين المستخدم من التحكم في بياناته.

قائمة المراجع

- Ayyash, M. (2023). The effect of perceived control of information and privacy risk on customers' purchasing intention in social commerce platforms: The moderating role of personal interest. Palestine Technical University Research Journal, 11(1), 151–164.
- Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. Information Systems Research, 17(1), 61–80.
- Hsu, C.-L., Liao, Y.-C., Lee, C.-W., & Chan, L. K. (2022). Privacy concerns and information sharing: The perspective of the U-shaped curve. Frontiers in Psychology, 13, 771278.
- Lăzăroiu, G., Neguriță, O., Grecu, I., Grecu, G., & Mitran, P. C. (2020). Consumers' decision-making process on social commerce platforms: Online trust, perceived risk, and purchase intentions. Frontiers in Psychology, 11, 890.

- Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns: The construct, the scale, and a causal model. *Information Systems Research*, 15(4), 336–355.
- Wang, S., Chen, Z., Xiao, Y., & Lin, C. (2021). Consumer privacy protection with the growth of AI-empowered online shopping based on the evolutionary game model. *Frontiers in Public Health*, 9, 705777.
- Li, J., Xiao, W., Zhang, Y., & Mou, J. (2026). The contextual and environmental antecedents of privacy risk perception and its heterogeneous effects on user behaviors. *Industrial Management & Data Systems*.

الملاحق

ملحق مقترح: محاور الاستبانة

1. مخاطر الخصوصية المدركة.
2. الثقة في المنصات الرقمية.
3. التحكم المدرك في المعلومات.
4. نية الإفصاح عن المعلومات الشخصية.
5. نية استخدام الخدمات الرقمية.