



مجلة إدارة الأعمال والدراسات الاقتصادية



موقع المجلة: www.asjp.cerist.dz/en/PresentationRevue/313/

النمذجة البنائية لمساهمة أبعاد الأمن السيبراني للبيانات في تحقيق رضا المستهلك الإلكتروني من خلال تعزيز الثقة كمتغير وسيط دراسة ميدانية لعينة من مستخدمي بطاقات الدفع الإلكتروني لبنك التنمية المحلية BDL بولاية غرداية

Constructive modeling of the contribution of the cybersecurity dimensions of data to achieving electronic consumer satisfaction by enhancing trust as a mediating variable

A field study of a sample of BDL e-payment card users in the state of Ghardaia

بوداود بومدين، *BoudaoudBoumediene¹, boumediene.boudaoud@univ-ghardaia.dz

دحو سليمان، DahouSlimane², dahou.slimane@univ-ghardaia.dz

صواق عبد القادر، SouagAbdelkader³, abdelkadersouag86@gmail.com

¹ أستاذ محاضر ب ، مخبر التطبيقات الكمية والنوعية ، جامعة غرداية (الجزائر)

² أستاذ محاضر أ ، مخبر التنمية الادارية للارتقاء بالمؤسسات الاقتصادية، جامعة غرداية (الجزائر)

³ باحث، مخبر التطبيقات الكمية والنوعية، جامعة غرداية (الجزائر)

تاريخ النشر: 2021/06/07

تاريخ القبول: 2020/12/30

تاريخ الإرسال: 2020/09/02

الكلمات المفتاحية

ملخص

تهدف هذه الدراسة إلى التعريف بمفهوم وأبعاد الأمن السيبراني، وتبيان مساهمته في تحقيق رضا المستهلك الإلكتروني من خلال تعزيز الثقة كمتغير وسيطي لدى عينة مستخدمي بطاقات الدفع الإلكترونية لبنك التنمية المحلية BDL بولاية غرداية مكونة من (214) مفردة، حيث تم استخدام منهجية نمذجة المعادلة الهيكلية (SEM) Structure Equation Modeling وذلك باستخدام تحليل المسار path analysis واختبار التأثير المباشر وغير المباشر لمتغيرات الدراسة واختبار صلاحية وصدق وثبات النموذج البنائي للدراسة باستخدام البرنامج الإحصائي Amos 22.

توصلت الدراسة إلى: وجود علاقة تأثير مباشرة لأبعاد الأمن السيبراني (احترام الخصوصية، التكنولوجيا المستخدمة، تتبع الأثر) في ثقة المستهلك الإلكتروني لدى عينة مستخدمي بطاقات الدفع الإلكترونية لبنك التنمية المحلية BDL بولاية غرداية، كما أثبتت الدراسة أن هناك علاقة تأثير مباشرة للثقة في تحقيق رضا المستهلك الإلكتروني، كما بينت الدراسة أيضا أن هناك علاقة تأثير مباشرة لأبعاد الأمن السيبراني (احترام الخصوصية، سرية البيانات، التكنولوجيا المستخدمة) في تحقيق رضا المستهلك الإلكتروني، بالإضافة إلى إثبات أن هناك علاقة تأثير غير مباشر لأبعاد الأمن السيبراني (احترام الخصوصية، التكنولوجيا المستخدمة، تتبع الأثر) في تحقيق رضا المستهلك الإلكتروني من خلال وجود الثقة كمتغير وسيط.

كما توصلت الدراسة الى اقتراح نموذج معدل لمساهمة أبعاد الأمن السيبراني في تحقيق رضا المستهلك

* البريد الإلكتروني للباحث المرسل: bb.boudaoud@gmail.com

الإلكتروني من خلال تعزيز الثقة كمتغير وسيطي بعد رفض كل من (بعد سرية البيانات وبعد التوافر والديمومة)

تصنيف JEL: G21؛D91؛C55؛M31

Abstract	Keywords
This study aims to introduce the concept and dimensions of cybersecurity, and clarify its contribution to achieving electronic consumer satisfaction by enhancing confidence as an intermediate variable among the sample of electronic payment card users of the BDL in Ghardaia Governorate consisting of (214) singles, where the methodology of modeling the structural equation was used (SEM) Structure Equation Modeling, using path analysis to test the direct and indirect impact of study variables and test the validity, validity and reliability of the structural model of the study using the statistical program Amos 22. The study found: The existence of a direct impact relationship for the dimensions of cybersecurity (respect for privacy, the technology used, tracing the impact) on electronic consumer confidence among the sample of electronic payment card users at BDL in Ghardaia, and the study also demonstrated that there is a direct impact relationship of confidence in achieving satisfaction The electronic consumer, as the study also showed that there is a direct impact relationship for the dimensions of cybersecurity (respect for privacy, data confidentiality, the technology used) in achieving electronic consumer satisfaction, in addition to proving that there is an indirect impact relationship for the dimensions of cybersecurity (respect for privacy, the technology used, Tracking impact) in achieving electronic consumer satisfaction by having confidence as an intermediate variable. The study also reached a proposal for a modified model for the contribution of the dimensions of cybersecurity in achieving electronic consumer satisfaction through enhancing confidence as an intermediate variable after rejecting both (after data confidentiality and after availability and permanence).	Cybersecurity, Electronic consumer satisfaction, Confidence, Big data, Electronic payment cards.

JEL Classification Codes: M31 ;C55 ;D91 ;G21

I. مقدمة:

أصبحت قضية الأمن السيبراني من التحديات الكبرى على الصعيدين الإقليمي والعالمي، لا سيما في ظل تنامي التهديدات الأمنية الإلكترونية سواء من جهة ارتفاع عدد الهجمات أو الأضرار الناجمة عنها. حيث قد شهدت عدة بلدان في الآونة الأخيرة اختراقات أمنية مقلقة استهدفت مؤسسات وشركات وحتى الأشخاص، أدت إلى سرقة بيانات حساسة وأسرار دول أو حجب الخدمات الإلكترونية الحيوية أو السطو الإلكتروني على البنوك أو تشويه مواقع الويب أو شنّ الهجمات الإلكترونية على البنية التحتية ووسائل الإعلام. والأخطر من ذلك سرقة المعلومات المصرفية.

ومن أجل مواجهة هذا الخطر المحدق أجريت عدة ندوات ودورات ومؤتمرات في مجال الأمن السيبراني بإثراء هذا الميدان بالتعاون مع العديد من المؤسسات والباحثين لتحقيق الأهداف المرجوة والمتمثلة في ضمان الأمن المعلوماتي وتوافر واستمرار عمل نظم المعلومات وسلامة الشبكات، بالإضافة إلى تعزيز حماية وسرية وخصوصية البيانات الشخصية خاصة تلك التي تتعلق بالمستهلك الإلكتروني في المجال الاقتصادي، الأمر الضروري الذي يفرض إيجاد الآليات والتدابير التي تحقق ثقة المستهلك ورضاه في مجال المعاملات الإلكترونية من خلال التجارة والتسويق والتسوق في الفضاء السيبراني

الجزائر من بين الدول التي ليست بمنأى عن التهديدات التي أفرزتها الثورة التكنولوجية الحديثة مما جعلها من بين أولوياتها في حماية أمن مجتمعها ومؤسساتها، خاصة تلك المؤسسات التي باشرت مجال الرقمنة والتعاملات الإلكترونية، وهو ما يدفعنا للبحث عن مدى توفر الأمن السيبراني في المؤسسات المصرفية الجزائرية التي تعتبر حديثة في مجال الرقمنة واستعمال بطاقات الدفع الإلكتروني، خاصة وأن الخدمات الإلكترونية التي تقدمها تتوقف أساسا على مدى أمنها

بالدرجة الأولى ومن ثم تحقيق أقصى إشباع ممكن للمستفيد منها وأعلى مستوى من الرضا لديه، لذلك أصبح لزاماً عليها طرح خدماتها الإلكترونية بصفة تتماشى ومتطلبات ورغبات المستهلكين، والتي من خلالها تستطيع التأثير فيهم واستهداف أكبر عدد ممكن وتحقيق رضاهم.

وانطلاقاً مما سبق يتبادر الإشكال المفاهيمي التالي:

"ما مدى تأثير الأمن السيبراني للبيانات في تحقيق رضا المستهلك الإلكتروني من خلال تعزيز الثقة لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية BDL بولاية غرداية؟

وتندرج تحت هذه الإشكالية الرئيسية، أسئلة فرعية تتمثل في الآتي:

- 1- هل هناك علاقة تأثير مباشرة ذات دلالة إحصائية للأمن السيبراني في ثقة المستهلك الإلكتروني لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية BDL بولاية غرداية؟
- 2- هل هناك علاقة تأثير مباشرة ذات دلالة إحصائية للثقة في رضا المستهلك الإلكتروني لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية BDL بولاية غرداية؟
- 3- هل هناك علاقة تأثير مباشرة ذات دلالة إحصائية للأمن السيبراني في رضا المستهلك الإلكتروني لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية BDL بولاية غرداية؟
- 4- هل هناك علاقة تأثير غير مباشرة ذات دلالة إحصائية للأمن السيبراني في رضا المستهلك الإلكتروني من خلال تعزيز الثقة لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية BDL بولاية غرداية؟

فرضيات البحث:

للإجابة على التساؤلات المطروحة سابقاً فإننا نستعين بفرضيات الدراسة التالية:

- H1:** هناك علاقة تأثير مباشرة للأمن السيبراني في ثقة المستهلك الإلكتروني.
- H2:** هناك علاقة تأثير مباشرة للثقة في رضا المستهلك الإلكتروني.
- H3:** هناك علاقة تأثير مباشرة للأمن السيبراني في رضا المستهلك الإلكتروني.
- H4:** هناك علاقة تأثير غير مباشرة للأمن السيبراني في رضا المستهلك الإلكتروني من خلال تعزيز الثقة.

أهداف البحث:

تهدف الدراسة من خلال الإجابة عن تساؤلات مشكلة الدراسة إلى ما يلي:

- معرفة طبيعة العلاقة المباشرة وغير المباشرة بين الأمن السيبراني للبيانات وتأثيرها على تحقيق رضا المستهلك الإلكتروني لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية BDL في ظل وجود الثقة كمتغير وسيطي.
- بناء نموذج نظري للعلاقات السببية بين متغيرات الأمن السيبراني ورضا المستهلك الإلكتروني وتعزيز الثقة.
- اختبار العلاقة السببية بين متغيرات الدراسة لفهم وتحليل مسارات العلاقات المتداخلة والمتكاملة المباشرة وغير المباشرة.
- قياس مستويات أبعاد الأمن السيبراني ورضا المستهلك الإلكتروني.

- تزويد متخذي القرار في المنظومة المصرفية بأهمية وفعالية اعتماد الأمن السيبراني بأبعاده (احترام الخصوصية، السرية، التوافر والديمومة، التكنولوجيا المستخدمة، تتبع الأثر) وتعزيز الثقة بما يحقق رضا المستهلكين الإلكترونيين.

أهمية البحث:

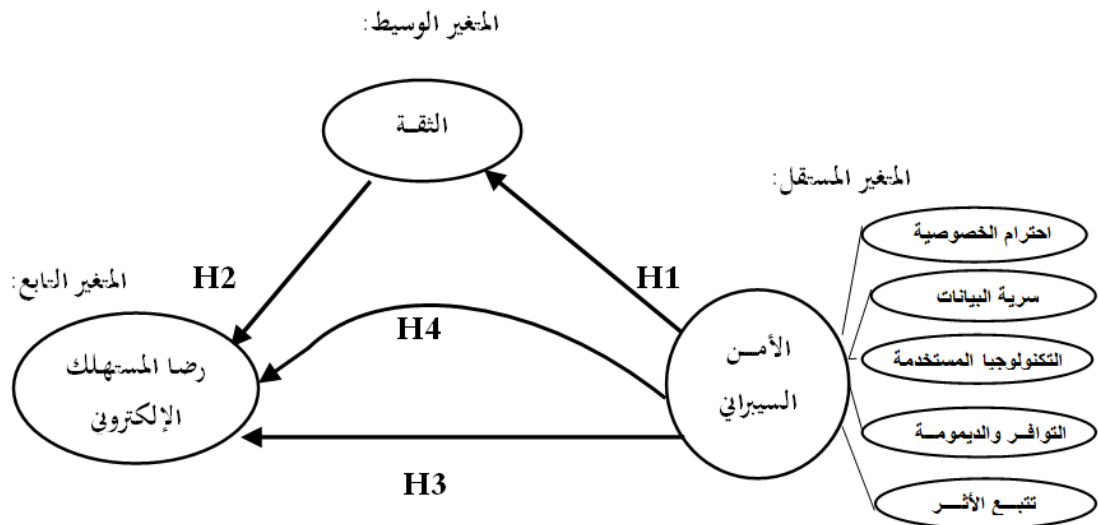
يستند الموضوع أهميته من كون أن الحكومات والمؤسسات بمختلف أنواعها وأحجامها هي تتجه نحو الاعتماد على التعاملات الإلكترونية، مما يجعلها عرضة لمخاطر عدة محلية أو حتى عابرة للحدود (تهديدات سيبرانية)، وهاته المخاطر هي تهدد استمرارية المؤسسات وأدائها. حيث يكتسي الموضوع أهمية بالغة نظرا لما يلي:

- أهمية قطاع البنوك في الوقت الراهن، حيث تمثل البنوك المحرك الأول لعمليات تمويل التنمية وما ينبغي النهوض بهذا القطاع وبالتالي فإن دراسة الأمن السيبراني للبنوك له أهمية كبيرة.
- عدم وجود دراسات ميدانية كافية اهتمت بالأمن السيبراني في البنوك التجارية الجزائرية وقياس مدى مساهمته في تحقيق رضا المستهلك الإلكتروني من خلال تعزيز الثقة.
- جاءت هذه الدراسة بمثابة دعوة إلى التطوير والاستمرارية والتفاعلية مع المستجدات وعدم الانتظار للتعرف على نتائج الآخرين لتقليدها، وإنما السعي للريادة والتعرف على كل ما هو جديد، لتحقيق الأسبقية والبقاء والاستمرارية.

متغيرات الدراسة:

- **المتغير المستقل: الأمن السيبراني** والمكون مما يلي:
(1- احترام الخصوصية، 2- سرية البيانات، 3- التكنولوجيا المستخدمة، 4- التوافر والديمومة، 5- تتبع الأثر).
- **المتغير الوسيط: الثقة.**
- **المتغير التابع: رضا المستهلك الإلكتروني.**

أنموذج الدراسة: يتضمن النموذج أو المخطط الافتراضي الموضح في الشكل التالي:
الشكل رقم: (1): أنموذج الدراسة الافتراضي.



المصدر: من إعداد الباحثين اعتمادا على الدراسات السابقة.

II. الدراسات السابقة

1. دراسة العتيبي عبد الرحمن بن بجاد شارع (2017):

بعنوان: "دور الأمن السيبراني في تعزيز الأمن الإنساني"، هدفت الدراسة إلى قياس وتحليل مدى توفر الأمن السيبراني بشركة أرامكو السعودية فرع منطقة الرياض، من خلال جاهزية عمالها في هذا المجال، حيث أن عدد مجتمع الدراسة 820 عامل وتم تجميع البيانات من خلال توزيع استبانة على عينة عشوائية بلغ حجمها 400 عامل بالحاسوب الآلي في مجال الأمن السيبراني بشركة أرامكو موزعين على 12 محطة، حيث اتبع الباحث المنهج الوصفي معتمداً على التحليل واختبار الاستبانة والمقابلة لجمع المعلومات اللازمة من الموظفين والقادة، مع تحليلها باستخدام (spss). توصلت الدراسة إلى مجموعة من النتائج أبرزها: أن الإجراءات الفنية أو التقنية لحماية الفضاء السيبراني للشركة متوفرة بدرجة كبيرة، حيث يتم قفل النظام آلياً في حالة عدم استخدامه لفترة زمنية محددة أو في حالة وجود الخطر، بالإضافة إلى استخدام تقنيات تكنولوجية عالية كالمقاييس الحيوية (بصمة العين، الإصبع، الصوت) لمرور المصرح لهم، وأن سياسات الأمن السيبراني في الشركة متوفرة بدرجة كبيرة حيث تضمن الأنظمة آلية فعالة للإبلاغ عن أي محاولات للاختراق.

خلصت الدراسة إلى مجموعة من التوصيات، تتمثل بضرورة إتباع الوسائل العلمية والعملية لحفظ الأمن السيبراني للمؤسسات والشركات الحكومية والخاصة، وكذا ضرورة توحيد الجهود الاجتماعية والثقافية لبناء حصن منيع يحفظ الدولة وأمنها السياسي والاقتصادي والسيبراني، والعمل على المزيد من التعمق في دراسة مجال الأمن السيبراني والأمن الإنساني.

2. دراسة يوسف بوغرة (2017)

بعنوان: "الأمن السيبراني الاستراتيجية الجزائرية للأمن والدفاع في الفضاء السايبري"، هدفت الدراسة إلى معرفة مدى فعالية الإصلاحات الجزائرية في تحقيق مستوى عالي من الأمن السيبراني في الفضاء السيبراني، حيث اتبع الباحث المنهج الوصفي من خلال عرض وتحليل نماذج من القوانين والمعاهدات الدولية بخصوص الجرائم السيبرانية، وكذا المنهج المسحي (التاريخي) بسرد بعض الوقائع والأحداث المتعلقة بموضوع البحث، والوقوف على المواقف ذات العلاقة. توصلت الدراسة إلى مجموعة من النتائج أبرزها: أن متغير الأمن السيبراني هو بعد مفاهيمي يكتنفه الكثير من الجهود الأكاديمية لتحقيقه في العالم الافتراضي وذلك لما يواجهه من صعوبات وعوائق من بينها تباين الوسائل وتكنولوجيا الأنظمة المعلوماتية ووجود ثغرات سيبرانية (تقنية وقانونية)، وأن دولة الجزائر استطاعت إلى حد ما وضع إصلاحات في مجال الأمن السيبراني تداركاً للأخطاء والانعكاسات المترتبة عن تفعيل الإدارة الإلكترونية ولوج العالم الافتراضي لكن ليس بصفة مطلقة نظراً للتعقيد الشائب في هذا الفضاء مع تعدد الفواعل.

خلصت الدراسة إلى مجموعة من التوصيات المهمة، تتمثل بضرورة تعزيز جيل من الموارد البشرية ذات كفاءة قصوى ومستوى عالي مع البقاء على إطلاع بالنماذج الحديثة لأنظمة المعلومات وتكنولوجيا الأمن السيبراني، كما أن تحقيق الأمن وإرساء الثقة في الفضاء السيبراني شرطاً أساسياً لتسخير تقنيات المعلومات والاتصال في كافة مجالات التنمية (الاجتماعية، السياسية، الاقتصادية... الخ)، بالإضافة إلى أنه في عالم الأمن السيبراني لا يمكن الحديث عن ضمان تأمين مطلق للأنظمة لأن الأمر يتعلق بمسار للتطوير المستمر للأمن وبهذا كسب رهان الأمن السيبراني يستلزم تحديد مقاربة استباقية وتفاعلية.

3. دراسة William Crumpler (2018)

بعنوان: "The cybersecurity workforce gap in the commercial companies" "الأمنالسيبراني وفجوة القوى العاملة في الشركات التجارية"، هدفت الدراسة إلى إلقاء الضوء على التحدي الذي تواجهه الشركات التجارية في تجنيد القوى العاملة الماهرة في مجال الأمن السيبراني من أجل حماية أنظمتها ضد التهديدات الخبيثة، فاتبع الباحث المنهج الوصفي مستخدماً المقابلة لأرباب عمل 36 شركة تجارية في الولايات المتحدة الأمريكية. توصلت الدراسة إلى مجموعة من النتائج أبرزها: أن 82% من أرباب العمل يبلّغون عن نقص في مهارات الأمن السيبراني، و 71% أن فجوة القوى العاملة تسبب أضراراً مباشرة لمنظمتهم. خلصت الدراسة إلى مجموعة من التوصيات، أهمها أن الحاجة الأكبر هي للمهنيين ذوي التدريب الفني العميق في مجال الأمن السيبراني القادرين على القيام بأدوار عالية القيمة كتصميم النظام الآمن وتطوير الأدوات واختبار الاختراق، لذا على الشركات أن تبني علاقات مع مدربين ذو خبرة لتوصيل احتياجات القوى العاملة وفجوات المهارات.

4. دراسة Jeffrey Esinash (2015)

بعنوان "Factor affecting cybersecurity effectiveness in company Garmin" "العوامل المؤثرة في فعالية الأمن السيبراني في شركة (Garmin) الخاصة بالتكنولوجيات البحرية بأولاثكانساس بأمريكا". تهدف هذه الدراسة إلى معالجة العوامل المؤثرة في الأمن السيبراني من خلال دراسة حالة الشركة بمحاولة قياس أثر السياسات الأمنية على الفاعلية الأمنية المتبعة من قبل الشركة، حيث اتبع الباحث المنهج الوصفي مستعملاً الاستبيان تم توزيع 130 استبيان على مجتمع الدراسة المستهدف المتمثل في جميع موظفي الشركة المستخدمين لأجهزة الحاسوب 2015. وقد خلصت الدراسة إلى مجموعة من النتائج، أهمها أن دعم الإدارة العليا للسياسات الأمنية للأمن السيبراني وتدريب المستخدمين وزيادة الوعي، يؤثران على فعالية الأمن السيبراني للشركة لكن بدرجات مختلفة، حيث يزداد تأثير العوامل الثلاثة بقوة مقارنة بعامل دعم الإدارة العليا.

5. دراسة Robert Knake (2010)

بعنوان: "The impact of cyberspace threats on national security United States of America - Model" "أثر التهديدات السيبرانية على الأمن القومي الولايات المتحدة الأمريكية - نموذجاً"، هدفت الدراسة إلى توضيح العلاقة بين الأمن السيبراني والأمن القومي علاقة التأثير والتأثر مع إبراز إسهامات وجهود الدول وخاصة الولايات المتحدة الأمريكية في مواجهة التهديدات السيبرانية. اتبع الباحث المنهج الوصفي من أجل تفسير ظاهرة التهديدات السيبرانية وتحديد خصائصها، وكذا وصف طبيعة العلاقة بين الأمن السيبراني في العالم بشكل عام والولايات المتحدة الأمريكية بشكل خاص، وصولاً إلى تحليل وتفسير. توصلت الدراسة إلى مجموعة من النتائج أبرزها: أن التهديدات السيبرانية لها طبعها التقني الخاص، إضافة إلى أنها تهديدات عابرة للحدود، تهدد سيادة الدول، وعليه فالمواجهة تكون على مستويين، الأول تقني والثاني قانوني بتعاون دولي. بالإضافة إلى أنه رغم قوة الولايات المتحدة الأمريكية سيبرانيا فهي تواجه تهديدات وصراع في الشبكات أي في الفضاء السيبراني خاصة من الصين وروسيا، بما قد يهدد أمنها القومي.

خلصت الدراسة إلى مجموعة من التوصيات، أهمها أن فهم وإدراك أن الأمن السيبراني عنصر رئيس في الأمن القومي ككل، وله علاقة وطيدة مع قضايا التنمية السياسية والاجتماعية والاقتصادية، وضرورة إدماجه في العقيدة الأمنية للدولة، ووضع استراتيجية سيبرانية واضحة، بالإضافة إلى ضرورة وضع وتحديث الأجهزة التقنية ومواكبة التكنولوجيا وكذا

تحديث التشريعات القانونية التي تنظم وتؤطر الفضاء الإلكتروني، مع ضرورة التعاون الدولي بين جميع الفاعلين لترسيخ قواعد السلوك الجيد ونشر قيم وثقافة الفضاء السيبراني السلمي والأمن.

III. الإطار النظري والمفاهيمي للدراسة

يعتبر الأمن السيبراني من بين العوامل الرئيسية لنجاح المؤسسات ولذا لكتعتها المؤسسات الخدمية والسلعية اهتماما كبيرا بهدف أمان منتجاتها وخدماتها المقدمة، ومنه فهي تسعى إلى الحرص على سلامة مختلف المعاملات الإلكترونية في الفضاء السيبراني*، وهذا لمواجهة التحديات والتطورات في مجال الأنترنت والإلكترونيات سيما منها التلبيبة حاجات ورغبات زبائنهم من خلال كسب ثقتهم ومن ثم كسب رضاهم وولائهم.

ماهية الأمن السيبراني (Cyber Security)

أولا: تعريف الأمن السيبراني (Cyber Security):

يعتبر مصطلح الأمن السيبراني Cyber Security واحدا من المصطلحات التي تعرفت عدد فيا التعريفات المقدمة له، فمصطلح حسيبار Cyber هو لفظ يوناني الأصل، مشتق من كلمة Kybernetes؛ بمعنى القيادة أو التحكم، مصدرها Cybernetics يعني: "علم الاتصالات وأنظمة التحكم الآلي في كل من الآلات والأشياء الحية"، حيث قدمت وزارة الدفاع لولايات المتحدة الأمريكية تعريفا لمصطلح الأمن السيبراني، أين "جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بتجميع أشكالها (الإلكترونية والمادية) من مختلف الجرائم، الهجمات، التخريب، والتجسس، والحوادث" (Ventre, 2011, p. 103).

يمكن تعريف الأمن السيبراني بأنه: "أمن الشبكات والأنظمة المعلوماتية والبيانات والمعلومات والأجهزة المتصلة بالإنترنت وعليه فهو المجال الذي يتعلق بإجراء اتوماتيكية معايير الحماية المفروضة اتخاذها، أو الالتزام بها لمواجهة التهديدات ومنع التعديات، للحد من آثارها فإقصى وأسوأ الأحوال. ويرتبط هذا الأمر بتباطؤ وثيق بأمن المعلومات والبيانات. فالوصول لهذه الأخيرة أو بثها، الاطلاع عليها والمتاجرة فيها، أو تشويهها واستغلالها، هو ما يفتقر غالبا لأحيان وراء عمليات الاعتداء على الشبكات، وعلى الأنترنت. (جبر، 2017، صفحة 26)

بينما عرّف المشرع الجزائري الأمن السيبراني على أنه: "مجموع الأدوات والسياسات ومفاهيمها لأمنها لآليات أمنية والمبادئ التوجيهية وطرق الضمانات التكنولوجية التي يمكن استخدامها في المساس بتوفر وسلامة وسرية البيانات المخزنة أو المعالجة والمرسلة" (الجريدة الرسمية، 2018، صفحة 7)

ثانيا: مفهوم البيانات الشخصية:

* **البيانات (Data):** هي: "جميع المصطلحات، والرموز، والأرقام، والصور، والحروف، والإشارات، والكلمات، أو خليط منها جميعا أو بعض منها التي لا علاقة بين بعضها البعض، ولم تخضع بعد للتفسير أو التجهيز للاستخدام، ليس لها دلالات أو معنى محدد، والتي تدخل في النظام المعلوماتي بشكل معين، لتحويلها للمعلومة، فهي المادة الأساسية للمعلومات" (عطية، 2009، صفحة 38).

فهو: "حقائق أولية Raw Facts وعناصر أو مادة خام Raw، وتعني معطيات لم تُعالج يدويا أو حاسوبيا لاستنباط معانيها واستجلاء سياقها العام أو مضمونها أو محتواها" (ياسين، 2010، صفحة 21).

*البيانات الشخصية: هي: "البيانات العائدة إلى شخص معين، والتي يمكن أن تساعد على تحديد هويته، والتعرف إليه، كالاسم الشخصي، وعنوان السكن، ورقم الهاتف، والبريد الإلكتروني، ورقم السيارة، وغيرها" (جبور، 2017، صفحة 189).

ثالثاً: أهداف الأمن السيبراني:

- تأمين الفضاء الإلكتروني بما فيه الخدمات الرقمية.
- الحفاظ على سرية المعلومات وقصر النفاذ على الجهات المصرح لها فقط.
- الحفاظ على سلامة البيانات والبرامج وعدم فساد حالتها.
- الحفاظ على توافر تقديم الخدمات بشكل مستمر وبدون انقطاع أو تدهور.
- احترام الخصوصية الرقمية للمستخدمين والمتعاملين الإلكترونيين.
- ضمان الصدق في التصرفات الإلكترونية والاستدلال على الفاعل من خلال تتبع الأثر.
- الوصول إلى الوضع الأمثل لأداء نظام المعلومات جنباً إلى جنب مع مستوى أداء الأمن المطلوب
- تطوير السياسات والإجراءات الأمنية اللازمة للمنظمات والدول ونمو اقتصادها.
- خلق الثقة في التطبيقات والخدمات المقدمة خاصة في المعاملات التجارية والمالية إلكترونياً.
- المساعدة على حماية أصول وموارد المنظمات من النواحي التنظيمية، والبشرية، والمالية، والتقنية، والمعلوماتية حيث تتمكن من أداء مهامها بصفة جيدة.
- تعزيز قدرات التكنولوجيا لحماية المصالح الحيوية للدولة وأمنها الوطني والبنى التحتية الحساسة والقطاعات ذات الأولوية والخدمات الرقمية.
- اتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين على حد سواء من المخاطر المحتملة في مجالات استخدام الإنترنت المختلفة. (IUT، 2009، صفحة 101)

أبعاد ومستويات الأمن السيبراني:

أبعاد الأمن السيبراني:

يمكننا تعريف أبعاد الأمن السيبراني للبيانات بأنها مجموعة العناصر الواجب توافرها لحماية هاتهن البيانات، بحيث يُغطي كل عنصر من هذه العناصر جانباً من جوانب الحماية المطلوبة فتتكاملهذه العناصر تحت توفير الحماية وفي حال فقد أي منها سيكون هناك خلل لأمني، وللحفاظة على أمن البيانات في التطبيق والنظام يجب أن تتوفر خمسة عناصر هي:

1- احترام الخصوصية (Privacy):

تعتبر حق المستهلك الإلكتروني في عدم نشر أو بث بياناته الشخصية التي تتعلق بتعاملاته أو بحياته الخاصة، ويتم ذلك بداية من طلب كلمة السر خاصة به عند تسجيل حساب على الموقع الرئيسي الخاص بالبنوك التجارية والمعاملات الخاصة ببطاقات الدفع الإلكترونية. وهناك عدة حلول تكنولوجية جارية استخداماً لتحقيق عملية خصوصية البيانات والمعلومات الشخصية للمستهلك.

من المفروض أن سياسة الخصوصية هي تبنّي تعزيز ثقة الزبون في المتجر الإلكتروني، ومستوى هذه الثقة يؤثر في حجم نوعية البيانات التي يحصل عليها المتجر الإلكتروني، والمستهلك لا يقدم بياناته ومعلوماتها للمتجر الإلكتروني إلا من أجل الحصول على قيمة، حيث أن المتجر الإلكتروني يسعى إلى الحصول على البيانات والمعلومات الدقيقة ذات المصدقية، ولا يتحقق هذا إلا بتحقيق ثقة الزبون في المتجر الإلكتروني.

2- سرية البيانات (Confidentiality):

إن سرية البيانات الشخصية والسرية الرقمية هي من حقوق الإنسان الأساسية، فهي تعني الحفاظ على سرية البيانات وتدفق المعلومات والمعاملات والخدمات أو الإجراءات التي تجري في الفضاء السيبراني ومنع الوصول إلى البيانات إلا لأشخاص المصرح لهم فقط.

وتعني أيضا الحفاظ على المعلومات والبيانات من أن يُطلع عليها، حيث يمكن تنفيذ السرية عن طريق مراقبة النفاذ والتشفير. حيث أن التشفير يساعد على حماية البيانات أثناء تخزينها أو معالجتها أو عند نقلها عبر وسائل الاتصال. (القحطاني، 2015، صفحة 91)

3- التكنولوجيا المستخدمة (Technology Used):

يعني الخدمة التي من خلالها يمكن الحفاظ على المعلومات والبيانات من التعديل أو الحذف أو الإضافة أو إعادة التركيب أو التوجيه طالما أنها إلكترونية، وهذا بفضل دقة الأنظمة المعالجة لها وسلامتها من التلاعب أو التغيير ويتطلب ذلك أن تعمل الأجهزة والبرامج وأنظمة الشبكات بانسجام تام للحفاظ على المعلومات والبيانات ومعالجتها ونقلها ومراقبتها، وهذا الأمر من المفروض أن يولد الثقة لدى المتعامل. وللحيلولة دون التلاعب، يلزم وجود طريقة للتصديق على أنها لم تتعرض للتعديل أثناء الخزن أو النقل.

بالإضافة إلى سلامة ومتانة البنية التحتية من خلال وجود المعدات التكنولوجية والأجهزة الفنية التي توفر الحماية التقنية ضد الأعطال والقصور في الموارد الأصلية وغالبا ما تعمل هذه المكونات بشكل آلي دون التدخل البشري.

4- التوافر والديمومة (Availability):

خدمة التوافر هي الخدمة التي تحمي النظام ليبقى متاحا دائما وهي موجهة خصيصا إلى أي خلل أو هجوم يمكن أن يؤدي إلى عدم التوافر، ومن الأمثلة على ذلك هجوم الفيروسات وهجمات حجب الخدمة أو منعها (Denial of Service-DoS) ويتطلب هذا في غالب الأحيان الحماية المادية التقنية، والهدف العام من عنصر التوافر والديمومة هو أن تكون الشبكة والأجهزة والأنظمة والبرامج والخدمات متاحة في جميع الأوقات التي يحتاج إليها المستخدم لتأمين توافر الخدمات والنظم والبيانات، يجب تحديد الأحجام المناسبة لنظم البنية التحتية، وتوفير الإدارة التشغيلية للموارد والخدمات. بمعني أن البيانات متوفرة للمستخدمين في أي وقت ومن أي مكان في أي وقت ومن أي مكان في أي وقت ومن أي مكان في أي وقت. (إدارة قواعد البيانات ووسائل الاتصال).

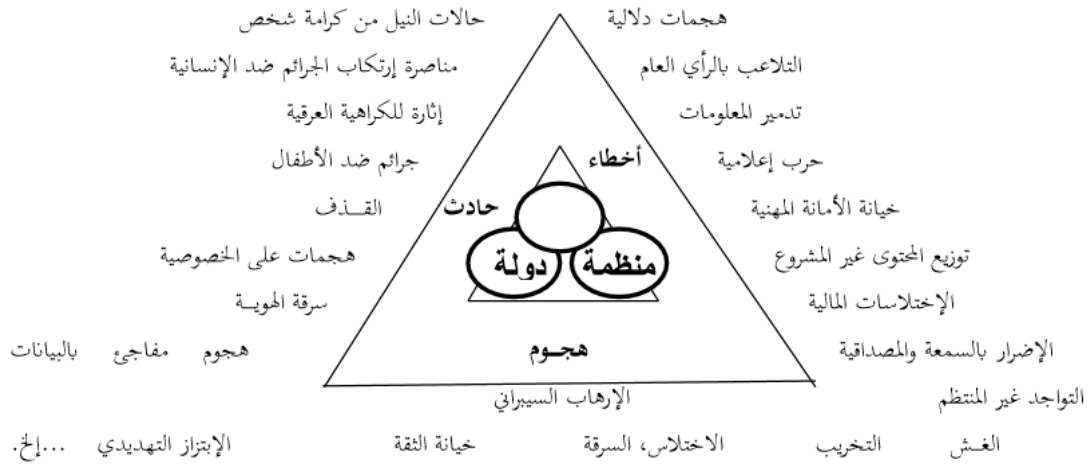
5- تتبع الأثر (Traceability):

هي الخدمة التي من خلالها تضمن عدم إنكار أي شخص قام بتصرف ما متصل بالبيانات أو مواقعها على سبيل المثال: إذا منحت جهة معينة صلاحية لجهة أخرى لشراء منتج معين ثم أنكرت بعد ذلك أنها منحت هذه الصلاحية فإن خدمة عدم الإنكار ستكشف ذلك، بمعنى توفر قدرة إثبات وقوع العملية التفاعلية.

وكذلك قدرة الاستدلال على الفاعل وإمكانية الاقتفاء والقابلية للمراجعة لتحديد المسؤولية، كما يفترض مسبقا وجود آليات للتحقق من العمليات والإجراءات الإلكترونية في أوقات وتواريخ معينة عن طريق إلحاق بصمة التاريخ والوقت ويسمى هذا بقابلية التدقيق لدى النظام.

ثانيا: مستويات الأمن السيبراني:

شكل رقم: (02): مستويات الأمن السيبراني.



المصدر: (IUT، 2009، صفحة 8).

يوضح الشكل رقم: (02) أن للأمن السيبراني ثلاثة مستويات بداية من أمن الفرد إلى أمن المنظمة وصولاً إلى أمن الدولة حيث هناك تهديدات ومخاطر متزايدة تخلفها استخدامات التكنولوجيا الحديثة خاصة تلك المرتبطة باستعمال الإنترنت كما هي واضحة في الشكل، فموضوعنا اليوم يتحدث عن الأمن السيبراني للبيانات المتعلقة بالمستهلك الإلكتروني (الفرد) يعني المستوى الأول في المثلث، وما يحيط به من مخاطر وتهديدات (تدمير المعلومات والبيانات، التخريب، سرقة أو انتحال الهوية، السرقة، الاختلاس المالي، الغش، توزيع المحتوى غير المشروع، خيانة الثقة... الخ) وبهذا قد بات لزاماً اعتماد سياسة أمنية تضع مسألة توفير الأمن السيبراني على رأس الأولويات والاستراتيجيات.

تحديات الأمن السيبراني:

التحديات التي يطرحها الفضاء السيبراني، مصدرها العالم الحقيقي حيث الأشخاص والخدمات التي تستخدم الإنترنت، فالأمن السيبراني يمس أمن الثروة الرقمية والثقافية للأفراد والمنظمات والدول، بل إن التحديات التي ينطوي عليها ذلك معقدة ويحتاج التصدي لها ضرورة توافر الإرادة السياسية اللازمة لتصميم وتنفيذ استراتيجية لتطوير بنى تحتية وخدمات رقمية بمعنى استراتيجية أمن سيبراني متماسكة وفعالة وقابلة للتحقق منها ومن إدارتها. كما يجب أن تكون الاستراتيجية جزءاً من نهج متعدد التخصصات (تفاعل عدة قطاعات)، مع وجود حلول جاهزة على المستوى التقني والقانوني والإداري والتنظيمي، فأمن البنية الأساسية الرقمية له تحدي جد هام يتمثل في بناء ثقة المستخدم أو المتعامل أو المستهلك الإلكتروني وتوليد النمو الاقتصادي المرغوب فيه، والذي يفيد المجتمع كافة.

إن تملك زمام رصد المعلومات الرقمية، وتوزيع السلع الغير الملموسة، وسد الثغرة الرقمية كلها مشاكل ذات طبيعة اقتصادية واجتماعية تستلزم شيئاً أكثر من مجرد إتباع نهج وحيد البعد وتكنولوجي بحث تجاه الأمن السيبراني (IUT، 2009، صفحة 9).

2. ثقة المستهلك الإلكتروني

إن النمو السريع في استخدام التكنولوجيا الحديثة وشبكة الإنترنت يحمل العديد من الفرص والمزايا التنافسية لكافة منظمات الأعمال بصفة عامة وللبنوك بصفة خاصة، فالعمليات عبر الإنترنت والعلاقات المتبادلة بين الأطراف تتطلب وجود عامل الثقة، فما مفهوم هذا الأخير وما أبعاده؟

1.2 ماهية الثقة (Confidence):

ركز الباحثون في تفسير مفهوم الثقة على أنها درجة إيمان وتقبل الفرد للقرارات والسياسات التي تضعها إدارة المنظمة، والتي تقوم بتنفيذها وإدارتها بشكل عادل لجميع الأطراف (Cherif-Benmiled, 2012, p. 5).

ولتوضيح أكثر لمفهوم "الثقة" تعرضنا لما تطرق إليه بعض باحثي التسويق، كما هو موضح في الجدول التالي رقم (02):

جدول رقم: (02): مفاهيم "الثقة" من منظور بعض باحثي التسويق.

إسم الباحث	مفهوم الثقة
Morgan and Hunt (1994)	تحدث الثقة عند امتلاك طرف ما ثقة (Confidence) في أمانة وصدق شريك التبادل.
Gefen (2000)	الثقة في التاجر على الإنترنت هي رغبة أحد الأطراف لجعل نفسه عرضة لأعمال الطرف الموثوق فيه وفقا للشعور بالأمان والضمان والموثوقية.
Ba and Pavlou (2002)	الثقة هي التقييم الشخصي لأحد الأطراف بأن الطرف الآخر سيؤدي عملية معينة وفقا لتوقعه في بيئة تتسم بعدم التأكد.
Salo and Karjaluoto (2007)	الرغبة للاعتماد على أمانة وقدرة وخصائص الشخص الموثوق فيه وقراره حتى ولو كانت النتيجة غير معروفة حاليا.

المصدر: (عبد الله، 2013، الصفحات 57-58)

نستنتج من خلال التعاريف السابقة أن: الثقة هي توقعات طرف معين أنه يمكن الاعتماد على طرف آخر في تحقيق نتائج مرغوبة.

2.2 أهمية الثقة:

للثقة أهمية جد كبيرة في عمليات التبادل سواء بالنسبة للمؤسسة أو للعميل نستخلصها كما يلي:

- توفير الارتياح في العمل والقرارات.
- تجعل علاقة التبادل مع الشريك طويلة ودائمة.
- الثقة مفتاح نجاح العلاقات التجارية لا سيما تلك التي تتميز بدرجة عالية من المخاطر حيث يمكن اعتبارها كشبكة أمان.
- الفائدة الرئيسية من الثقة هي رضا العميل ومن ثم ولائه الذي يؤدي بدوره إلى علاقة بعيدة المدى.
- من غير الممكن تقييم الخدمة قبل الاستهلاك الفعلي وهذا ما يجعل الثقة عامل قرار ذو قيمة. (Halliburton, 2010, pp. 2-4)

4.2 العوامل المفسرة للثقة في البحوث التسويقية:

اهتمت البحوث التسويقية كثيراً لعنصر الثقة كمتغير تسويقي مهم في بناء العلاقة بين المؤسسة والمستهلكين، حيث ظهرت تيارات فكرية تركز على المتغيرات المفسرة للثقة لما تكتسيه معرفة هذه العوامل من أهمية لدى المسوقين في سبيل كسب ثقة المستهلكين، تُظهر الدراسات أن هناك أربع أنواع للعوامل المفسرة للثقة وهي:

- **العوامل المرتبطة بالمؤسسة:** هي السمعة الحسنة للمؤسسة، الحجم الكبير للمؤسسة، خبرة المؤسسة، الاستثمارات الخاصة بالمؤسسة، سلطة أو قوة المؤسسة، الرضا: نادرة الدراسات التي تناولت العلاقة بين الرضا والثقة، وقد اختلف الباحثون في كون الرضا هو مصدر للثقة أم أن الثقة هي مؤشر للرضا، وعلى العموم فقد أُعْتُبر الرضا مؤشر للثقة وهو شعور ينبثق من الإحساس بالراحة والأمان.
- **العوامل المرتبطة بالبائع:** قدرات وإمكانات البائع العالية، تماثل البائع والزيون من خلال العلاقة الشخصية، خصائص شخصية البائع، تصرفات البائع من خلال تبادل المعلومات.
- **المتغيرات المرتبطة بالمستهلك:** التعود أو الاعتياد، الرضا: كلما زاد رضا المستهلك عن منتج ما زادت ثقته.
- **العوامل المرتبطة بالمنتج:** الخبرات والتجارب السابقة مع المنتج/العلامة، الجودة أو صورة الجودة للعلامة.

3. مفهوم رضا المستهلك الإلكتروني

إن دراسة سلوك المستهلك للخدمة المقدمة يمثل محوراً أساسياً في البحوث والدراسات التسويقية التي تقوم بها المؤسسة ذلك كونها تعتبر نقطة الارتكاز التي تدور عليها أنشطة المؤسسة، كما أن رضا المستهلك يعد أكثر المعايير أهمية خاصة عندما يكون توجه المؤسسة نحو التطوير وهناك حاجة المؤسسة لتحديد ما إذا كان المستهلكون راضون عن الخدمة التي تلونها أم لا، فـهـيـفي بحثاً عن الوسائل التي يمكنها من تحسين مستوى الرضا وكذا الإجابة عن هذا لا تعتمد الرضا لدى المستهلكين على عوامل كثيرة، حيث أصبح على المؤسسة أن لاكتفيتها تحقيق رضا المستهلك فقط بل عليها أن تقيسه لتعرف على درجته، ولأجل ذلك اعتمدت أساليب قياس رضا المستهلك (البحوث الكمية والكيفية).

تعريف المستهلك الإلكتروني:

هو: "كلمة يحصل بواسطتها التعاقد بالوسائل الإلكترونية على سلعة أو خدمة بمقابل أو بدون مقابل إشباع حاجته الشخصية أو حاجات الآخرين." (فقيه، 2013، صفحة 69)

المستهلك الإلكتروني هو: "الشخص الذي ينتقي ويشتري السلع والخدمات ومن ثم يستهلكها لإشباع حاجاته ورغباته عن طريق التعاقد بالوسائل الإلكترونية الحديثة" (الحازمي، 2006، صفحة 29).

تعريف الرضا (The satisfaction):

تسعى المنظمة إنتاجية كانت أم خدمية لتحقيق رضا زبائنهم، ذلك لأنها وجدت أصلاً من أجل تلبية حاجاتهم ورغباتهم من خلال تقديمها للمنتجات والخدمات، لذا تطرق أغلب الباحثين إلى هذا المفهوم كما يلي في الجدول الآتي:

جدول رقم: (02): مفاهيم " الرضا " وفق وجهة نظر بعض باحثي التسويق.

إسم الباحث	التعريف
Ahonen, 2000.	هو مقياس لمكانته في ثقافة المنظمة ويمتد تأثيره ليشمل التحسينات المستمرة لكافة أنشطتها.

الرضا يمثل قدرة المنظمة على جذب الزبائن، فهو يمثل شعور المستهلك بالسرور والارتياح عند مقارنة أداء المنتج الفعلي الذي حصل عليه، مع توقعاته التي يحملها عن هذا المنتج من قبل، فإذا كان أداء المنتج أقل من التوقعات، فإن المستهلك يكون غير راضٍ، أما إذا كان أداء المنتج أعلى من التوقعات، فإن المستهلك يكون مسروراً وراضياً عن المنتج.	Smart, 2001.
هو الشعور الإنساني بالسعادة أو خيبة الأمل المتولد من المقارنة بين أداء المنتج وأداء الخدمات المقارنة مع توقعاته.	kotler, Gary, 2005.
هو تقييم الزبائن لمنتج أو خدمة من جهة ما إذا كان هذا المنتج يلبي احتياجاتهم وتوقعاتهم ويشبعها.	Wilson et al, 2008.

المصدر: (شاهين، 2014/2013، صفحة 57)

نستنتج من خلال التعاريف السابقة أن: الرضا هو الحالة التي تتفوق فيها نتائج الخدمة المقدمة للمستهلك على توقعاته مما يؤدي ذلك إلى إعادة الطلب لنفس الخدمة.

كما عرّف رضا العميل المصرفي على أنه: "قدرة المصرف على إشباع العميل لحاجاته العملية ورغباته، وتحديد مدى قبوله للخدمات المصرفية، ووسائل تقديمها" (العدوان، 2015، صفحة 112)

أهمية رضا المستهلك:

يمكن تلخيص أهمية رضا المستهلك بالنقاط الآتية:

- 1- المستهلك الراضع عن خدمات المنظمة يشعر بالاستقرار النفسي من خلال تعامله مع معاناته المنظمة وهذا مهم.
- 2- الرضا يوفر الحافز لدى المستهلك ليكون وفياً وأكثر ولاً الذي يتعامل معه.
- 3- بمرور الوقت يصبح المستهلك الراضي وسيلة إعلانية للسلعة أو الخدمة ويساهم في تكوين قناعة ورضا لدى المستهلكين آخرين ومرتبين من خلال الإخبار والإعلام عن السلعة المميزة.
- 4- المستهلك الراضي عن الخدمة يكرر عملية الشراء، مما يعين تكرار تعاملاته، وبالتالي نشوء علاقة اتصال دائمة.
- 5- يحقق رضا المستهلك أهداف المنظمة، والتي تتمثل بالربحية من خلال الاحتفاظ بالعملاء، وزيادة المبيعات من خلال كسب عملاء جدد، وتخفيض التكاليف التسويقية من خلال الكلمة المنقولة إيجابياً عن المنظمة.
- 6- المستهلك الراضي سوف يتغاضى عن الأخطاء البسيطة، بل أنه سوف يساعد المنظمة في حل هاته المشكلات أو الأخطاء، ويقوم بإعلامها عن أي مشكلة أو خطأ محتمل الوقوع.
- 7- الرضا هو مقياس جودة الخدمة المقدمة.

مستويات الرضا:

من خلال ما تقدم، يتضح أن رضا المستهلك هو حالة من مستويات التوقعات والأداء المدرك وهناك ثلاث مستويات:

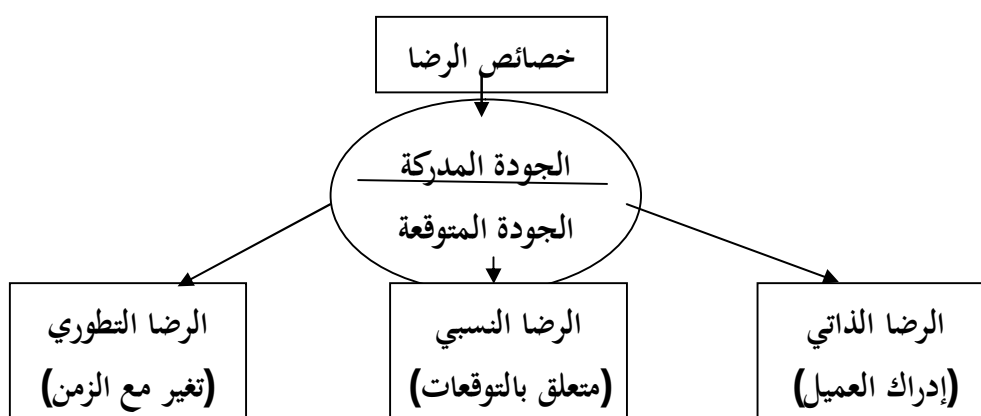
* أداء المنتج أكبر من التوقعات: فإنه سوف يشعر برضا عالي  تهلك أقل ميلاً للتحويل لمنافس آخر

*أداء المنتج يساوي التوقعات: فإنه سوف يشعر برضا متوسط ← المستهلك قابلاً للتحويل لمنافس آخر في حال كانت خدماتها أكثر جاذبية بالنسبة للعميل.

*أداء المنتج أقل من التوقعات: فإنه سوف يشعر بعدم الرضا ← هذا المستهلك يمكن أن يقوم بالاستغناء عن الخدمة أو ترك انطباعاً سلبي عن الخدمة في ذهنه.

خصائص الرضا:

الشكل رقم: (03): خصائص الرضا.



المصدر: (بوسطة، 2010/2011، صفحة 97).

توضيح خصائص الرضا كالآتي:

1- الرضا الذاتي: يتعلق برضا العميل بها بعنصرين أساسيين هما: طبيعة ومستوى التوقعات الشخصية للعميل من جهة، ولإدراك الذات للخدمة المقدمة من جهة أخرى، حيث إن العميل يحكم على الخدمة من خلال توقعاته الشخصية، وليس على أساس جودة الخدمة؛ لذا فإن العميل لا يحكم على الخدمة بشكل واقعي موضوعي، فالعميل الذي يحكم على الخدمة بأنها أفضل منا المنافسة سيقدِّرها عميلاً آخر أقل جودة، لذلك على المنظمة أن تقدم خدماتها بما يتوافق مع حاجات العملاء وتوقعاتهم، وبهذا تستطيع تحقيق رضا عملائها.

2- الرضا النسبي: لذلك العميل يقدِّر نسبياً، به، والعميل يقوم بالمقارنة من خلال نظرته لمعايير السوق من حيث: طبيعة المنتجات المطروحة، وأسعارها، البيئة المحيطة، وفي حال تلقي العميل للخدمة نفسها في البنك، يكون تقييمهما مختلفاً، وذلك كون توقعات كل منهما مختلفة عن الآخر حول الخدمة، وهذا الأمر يوضح أنها ليس من الضرورة أن تكون الخدمات الأفضل هي الأكثر ربحاً، بل إنَّ المعيار هنا توافق الخدمة مع توقعات العميل، ومدى تلبيتها لاحتياجاتها بشكل لا يرضيه.

3- الرضا التطوري: رضا العميل يتطور عبر الزمن من خلال مستوى التوقع من جهة ومستوى الإدراك من جهة أخرى، وذلك وفقاً للتطور الحاصل في رغباته وتغيُّرها، أو لوجود خدمات جديدة، أو بسبب المنافسة الشديدة بين المنظمات.

IV. الدراسة الميدانية لدى عينة عملاء بنك التنمية المحلية BDL بمدينة غرداية.

الإجراءات المنتهجة للدراسة الميدانية

مجتمع وعينة الدراسة:

اقتصرت عينة الدراسة على اجابة (214) مستهلك إلكتروني يتعامل بواسطة بطاقة الدفع الإلكتروني مع بنك التنمية المحلية BDL من مجتمع الدراسة البالغ عدده: (3500)، تم اختيارهم بطريقة عشوائية ميسرة، حيث تم توزيع 220 استبانة.

تصميم واختبار أداة الدراسة

1: تصميم الاستبانة: تم تصميم استبانة أعدت لغرض الدراسة شملت (44) سؤالاً مقسمة على أربعة أجزاء:

1-1 الجزء الأول: معلومات شخصية عامة حول المتغيرات الديموغرافية لعينة الدراسة من حيث: الجنس، الفئة العمرية، المستوى التعليمي، والمهنة والدخل، ومدة التعامل مع البنك: الفقرات (01-08).

1-2 الجزء الثاني: وشمل متغيرات الدراسة المستقلة، حيث خصص لمعرفة الأمن السيبراني وهي:

-احترام الخصوصية الفقرات (09-13)،

-سرية البيانات الفقرات (14-18)،

-التكنولوجيا المستخدمة الفقرات (19-23)،

-التوافر والديمومة الفقرات (24-28)،

-تتبع الأثر الفقرات (29-32)،

2) صدق وثبات أداة الاستبانة:**1-2 صدق المحكمين (الصدق الظاهري):**

يقصد بصدق أداة القياس مدى قدرة الاستبانة على قياس المتغيرات التي صممت لقياسها، ولهذا الغرض تم عرض الاستبانة على مجموعة من الأساتذة المحكمين في التخصص من جامعة غرداية وجامعة الأغواط ومن ذوي الاختصاص والخبرة الميدانية، وهذا للتعرف على آرائهم في مدى ملائمة الاستبانة للأهداف التي نرمي لتحقيقها من حيث سلامة اللغة ودقة العبارات، وقد تم إجراء تعديلات عليها بناء على توجيهاتهم، إلى أن استقرت على صورتها النهائية، وأعتبر موافقة غالبية المحكمين على الاستبانة مؤشراً على الصدق الظاهري للأداة.

2-2 ثبات أداة الدراسة:

يقصد بثبات أداة الدراسة مدى قدرة الأداة على إعادة إعطاء نتائج مماثلة إذا أعيد استخدامها في نفس الظروف وبشروط مماثلة.

1-2-2 اختبار ألفا كرومباخ:

للتأكد من ثبات أداة القياس المستخدمة في الدراسة تم احتساب معامل (ألفا كرونباخ) لأبعاد الدراسة باستثناء المعلومات والبيانات العامة، إذ أظهرت نتائج التحليل الإحصائي أن مستوى الثبات كان عالياً وفقاً للمعايير الإحصائية المتعارف عليها حيث بلغ 932، وهو ما يفوق 93% مما يجعل المعيار مقبول جداً.

الجدول رقم: (03): اختبار ألفا كرومباخ الكلي للفقرات

Statistiques de fiabilité

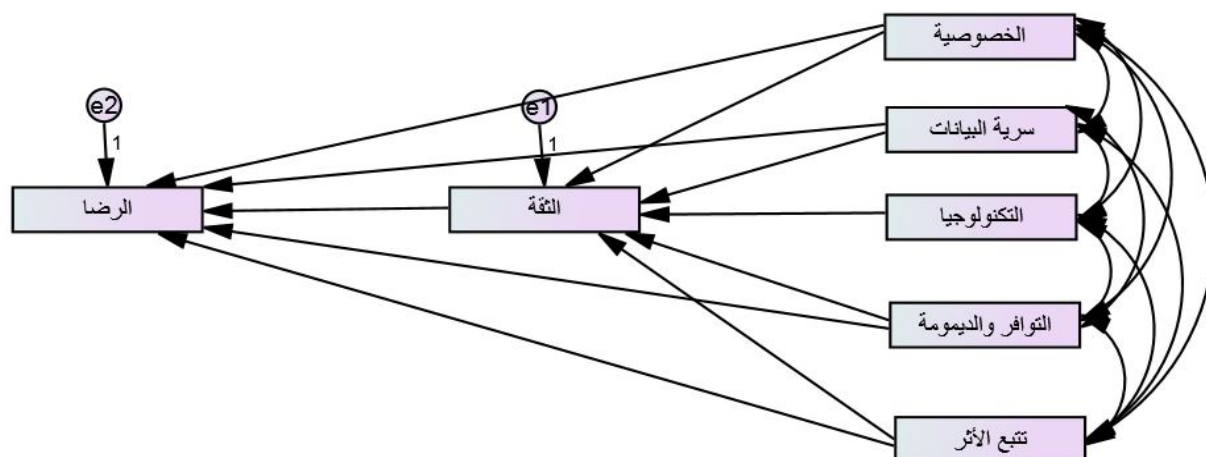
Alpha de Cronbach	Nombred'éléments
-------------------	------------------

36	,932
----	------

المصدر: من إعداد الباحثين بناء على مخرجات برنامج spss v23

ثانيا: النموذج النظري (العام) المقترح للدراسة:

الشكل البياني رقم: (04): النموذج النظري (العام) المقترح للدراسة



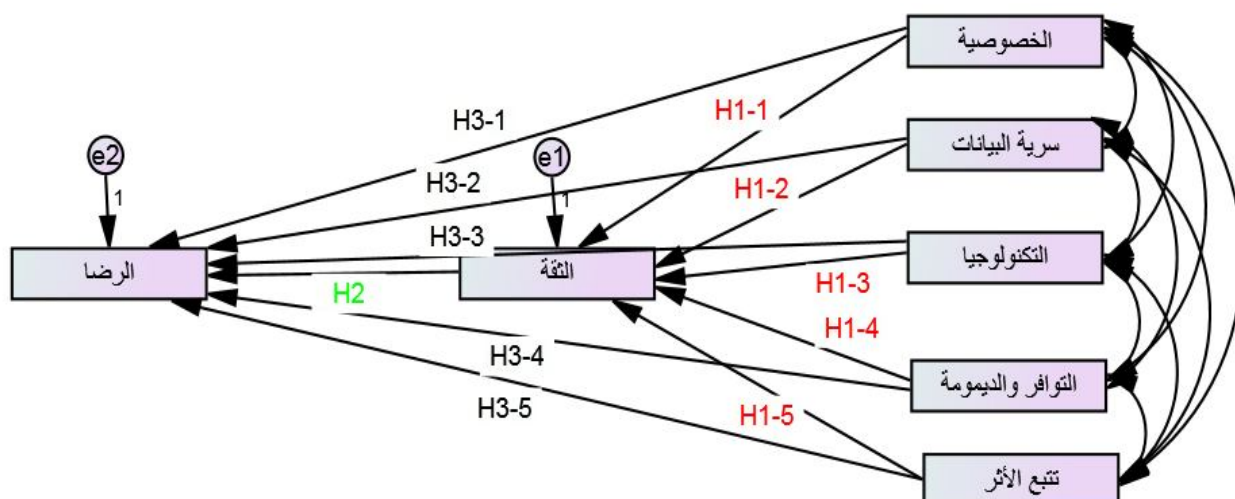
المصدر: من إعداد الباحثين بناء على مخرجات برنامج Amos v22

تحليل نتائج واختبار فرضيات الدراسة الميدانية

اختبار الفرضيات وتحليل مسارات العلاقات للنموذج العام للدراسة

يتم اختبار الفرضيات وتحليل مسارات العلاقات لنموذج الدراسة العام المقترح للإجابة على إشكاليات الدراسة المطروحة في الفصل السابق بناء على النموذج العام للدراسة النهائي الذي بين العلاقات المفروضة حسب الشكل البياني التالي:

الشكل رقم: (05): فرضيات الدراسة وفق النموذج العام النهائي للدراسة



المصدر: من إعداد الباحثين بناء على مخرجات Amos v22

من خلال النموذج العام للدراسة، سنحاول الإجابة على تساؤلات الدراسة المطروحة من خلال فرضيات الدراسة الآتية:

الفرع الأول: اختبار وتحليل مسار الفرضيات

أولاً: اختبار وتحليل مسار الفرضية الأولى:

H1 - هناك علاقة تأثير مباشرة للأمن السيبراني في ثقة المستهلك الإلكتروني.

وهذه الفرضية جاءت للإجابة على السؤال الفرعي الأول:

هل هناك علاقة تأثير مباشرة ذات دلالة إحصائية للأمن السيبراني في ثقة المستهلك الإلكتروني لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية BDL بولاية غرداية؟ ويمكننا الاستعانة بالفرضيات الفرعية التالية:

H1-1 - هناك علاقة تأثير مباشرة بين احترام الخصوصية وثقة المستهلك الإلكتروني.

H1-2 - هناك علاقة تأثير مباشرة بين سرية البيانات وثقة المستهلك الإلكتروني.

H1-3 - هناك علاقة تأثير مباشرة بين التكنولوجيا المستخدمة وثقة المستهلك الإلكتروني.

H1-4 - هناك علاقة تأثير مباشرة بين التوافر والديمومة وثقة المستهلك الإلكتروني.

H1-5 - هناك علاقة تأثير مباشرة بين تتبع الأثر وثقة المستهلك الإلكتروني.

1.1 اختبار الفرضيات الفرعية:

يلخص الجدول رقم: (04) مخرجات برنامج AMOS V22 لنتائج تحليل مسار العلاقة بين بعد أبعاد الأمن السيبراني وثقة المستهلك الإلكتروني المتوصل إليها من النموذج العام للدراسة كالتالي:

الجدول رقم: (04): نتائج تحليل مسار العلاقة بين أبعاد الأمن السيبراني وثقة المستهلك الإلكتروني

الفرضية	المتغير المستقل	المتغير الوسيط	التأثير المباشر	القرار
---------	-----------------	----------------	-----------------	--------

الفرعية		ثقة المستهلك الإلكتروني				الكلية
		معامل الانحدار	قيمة T	مستوى الدلالة	البواقي	
H1-1	احترام الخصوصية	0,207	2,098	***	0,08	0,207
H1-2	سرية البيانات	0,033	0,330	0,741	0,110	0,033
H1-3	التكنولوجيا المستخدمة	0,192	1,827	0,022	0,07	0,192
H1-4	التوافر والديمومة	-0,118	-1,354	0,176	0,08	-0,118
H1-5	تتبع الأثر	0,166	2,178	0,029	0,07	0,166

المصدر: من إعداد الباحثين بناء على نتائج برنامج Amos v22

ثانيا: اختبار وتحليل مسار الفرضية الثانية:

H2: هناك علاقة تأثير مباشرة للثقة في رضا المستهلك الإلكتروني.

وهذه الفرضية جاءت للإجابة على السؤال الثاني:

- هل هناك علاقة تأثير مباشرة ذات دلالة إحصائية للثقة في رضا المستهلك الإلكتروني لدى عينة مستخدمي

بطاقات الدفع الإلكترونية بينك التنمية المحلية BDL بولاية غرداية؟

من خلال نتائج الجدول رقم: (05) الذي يلخص مخرجات برنامج AMOS V22 لنتائج تحليل مسار العلاقة بين

بعد الثقة ورضا المستهلك الإلكتروني المستنتجة والمتوصل إليها من النموذج العام للدراسة كالتالي:

الجدول رقم: (05): نتائج تحليل مسار العلاقة بين بعد الثقة ورضا المستهلك الإلكتروني

المتغير التابع				المتغير الوسيط
رضا المستهلك الإلكتروني				
البواقي	مستوى الدلالة	قيمة T	معامل الانحدار	الثقة
0,02	***	13,919	0,402	
0,402				التأثير المباشر الكلي

المصدر: من إعداد الباحثين بناء على نتائج برنامج Amos v22

تشير النتائج إلى وجود علاقة ارتباطية موجبة بين بعد الثقة ورضا المستهلك الإلكتروني، حيث بلغت قيمة معامل

الانحدار: 0,402، مع قيمة ت الحرجة قدرها: 13,919، وبمستوى دلالة: 0,000، كما أن بواقي العلاقة بين بعد الثقة

ورضا المستهلك الإلكتروني قدرها: 0,02.

وعليه فإنه يتم قبول صحة الفرضية (H2) التي تنص على:

هناك علاقة تأثير مباشرة بين الثقة ورضا المستهلك الإلكتروني.

ثالثا: اختبار وتحليل مسار الفرضية الثالثة:

H3: هناك علاقة تأثير مباشرة للأمن السيبراني في رضا المستهلك الإلكتروني.

وهذه الفرضية جاءت للإجابة على السؤال الرئيسي الثالث:

- هل هناك علاقة تأثير مباشرة ذات دلالة إحصائية للأمن السيبراني في رضا المستهلك الإلكتروني لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية BDL بولاية غرداية؟
ويمكننا الاستعانة بالفرضيات الفرعية التالية:

- **H3-1:** توجد علاقة تأثير مباشرة بين احترام الخصوصية ورضا المستهلك الإلكتروني.
- **H3-2:** توجد علاقة تأثير مباشرة بين سرية البيانات ورضا المستهلك الإلكتروني.
- **H3-3:** توجد علاقة تأثير مباشرة بين التكنولوجيا المستخدمة ورضا المستهلك الإلكتروني.
- **H3-4:** توجد علاقة تأثير مباشرة بين التوافر والديمومة ورضا المستهلك الإلكتروني.
- **H3-5:** توجد علاقة تأثير مباشرة بين تتبع الأثر ورضا المستهلك الإلكتروني.

1. اختبار الفرضية الفرعية الأولى:

H3-1: هناك علاقة تأثير مباشرة بين احترام الخصوصية ورضا المستهلك الإلكتروني.

يلخص الجدول رقم: (06) مخرجات برنامج AMOS V22 لنتائج تحليل مسار العلاقة بين بعد احترام الخصوصية ورضا المستهلك الإلكتروني المتوصل إليها من النموذج العام للدراسة كالتالي:

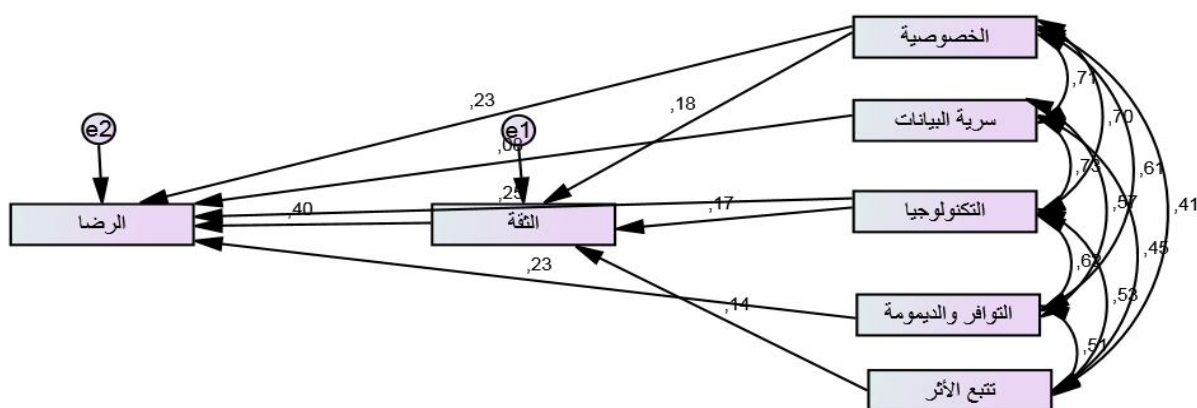
الجدول رقم: (06): نتائج تحليل مسار العلاقة بين أبعاد الأمن السيبراني ورضا المستهلك الإلكتروني

القرار	التأثير المباشر الكلي	المتغير التابع رضا المستهلك الإلكتروني				المتغير المستقل	الفرضية الفرعية
		البواقي	مستوى الدلالة	قيمة T	معامل الانحدار		
مقبولة	0,236	0,03	***	5,572	0,236	احترام الخصوصية	H1-1
مقبولة	0,93	0,047	0,048	1,976	0,93	سرية البيانات	H1-2
مقبولة	0,249	0,04	***	5,698	0,249	التكنولوجيا المستخدمة	H1-3
مقبولة	2,32	0,036	***	6,490	2,32	التوافر والديمومة	H1-4
مرفوضة	-0,041	0,032	0,205	-1,276	-0,041	تتبع الأثر	H1-5

المصدر: من إعداد الباحثين بناءً على نتائج برنامج Amos v22

من هنا بينت تقديرات مؤشرات نموذج الدراسة ما يلي:

- ✓ رفض العلاقة بين سرية البيانات وثقة المستهلك الإلكتروني، ذلك لكون العلاقة غير معنوية ($p\text{-value}=0,741$)
 - ✓ رفض العلاقة بين التوافر والديمومة وثقة المستهلك الإلكتروني ذلك لكون العلاقة غير معنوية ($p\text{-value}=0,176$)
 - ✓ رفض العلاقة بين تتبع الأثر ورضا المستهلك الإلكتروني، ذلك لكون العلاقة غير معنوية ($p\text{-value}=0,205$).
- عليه، قمنا بحذف العلاقات غير المعنوية لقياس العلاقات غير المباشرة، حسب نموذج المعدل التالي:
- الشكل البياني رقم: (06): النموذج النظري المعدل لقياس العلاقات غير المباشرة



المصدر: من إعداد الباحثين بناءً على نتائج برنامج Amos v22

رابعاً: اختبار وتحليل مسار الفرضية الرابعة:

H4: هناك علاقة تأثير **غير مباشرة** لأبعاد الأمن السيبراني في رضا المستهلك الإلكتروني من خلال تعزيز الثقة.

وهذه الفرضية جاءت للإجابة على السؤال الرابع:

- هل هناك علاقة تأثير **غير مباشرة** لأبعاد الأمن السيبراني في رضا المستهلك الإلكتروني من خلال تعزيز الثقة لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية BDL بولاية غرداية؟
ويمكننا الاستعانة بالفرضيات الفرعية التالية:

H4-1: هناك علاقة تأثير غير مباشرة بين احترام الخصوصية ورضا المستهلك الإلكتروني في ظل وجود الثقة كمتغير وسيطي.

H4-2: هناك علاقة تأثير غير مباشرة بين سرية البيانات ورضا المستهلك الإلكتروني في ظل وجود الثقة كمتغير وسيطي.

H4-3: هناك علاقة تأثير غير مباشرة بين التكنولوجيا المستخدمة ورضا المستهلك الإلكتروني في ظل وجود الثقة كمتغير وسيطي.

H4-4: هناك علاقة تأثير غير مباشرة بين التوافر والديمومة ورضا المستهلك الإلكتروني في ظل وجود الثقة كمتغير وسيطي.

H4-5: هناك علاقة تأثير غير مباشرة بين تتبع الأثر ورضا المستهلك الإلكتروني في ظل وجود الثقة كمتغير وسيطي.

اختبار الفرضيات الفرعية:

سنقوم بتبيان وحساب العلاقة غير المباشرة بين أبعاد الأمن السيبراني ورضا المستهلك الإلكتروني بوجود الثقة كمتغير وسيط كآتي:

الجدول رقم: (07): نتائج تحليل المسار للعلاقة غير المباشرة بين أبعاد الأمن السيبراني ورضا المستهلك الإلكتروني بوجود الثقة كمتغير وسيط

الفرضية الفرعية	المتغير المستقل	المتغير الوسيط		المتغير التابع		التأثير الكلي	القرار
		تأثير مباشر	تأثير غير مباشر	تأثير مباشر	تأثير غير مباشر		
H4-1	احترام الخصوصية	0,81	-	-	0,402	0,072	مقبولة
H4-2	سرية البيانات	0,00	-	-	0,402	0,00	مرفوضة
H4-3	التكنولوجيا المستخدمة	0,174	-	-	0,402	0,069	مقبولة
H4-4	التوافر والديمومة	0,00	-	-	0,402	0,00	مرفوضة
H4-5	تتبع الأثر	0,141	-	-	0,402	0,56	مقبولة

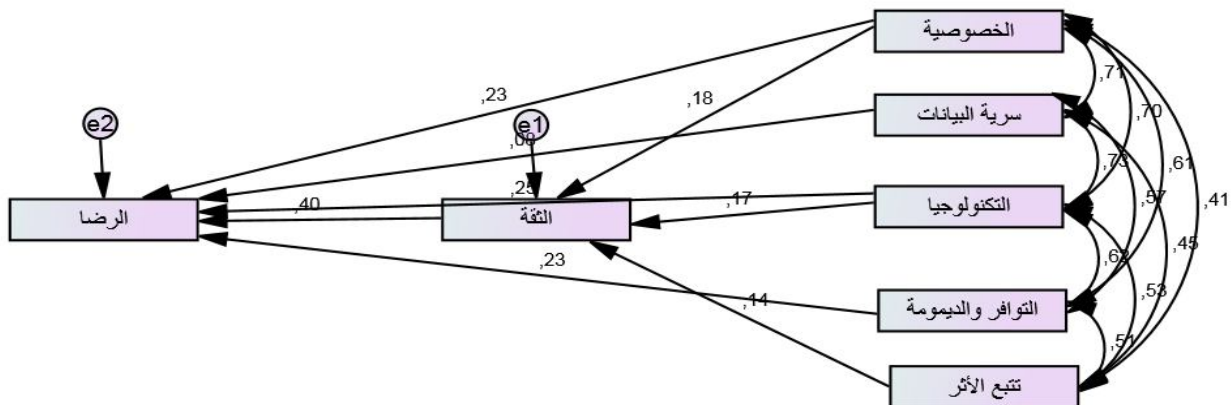
المصدر: من إعداد الباحثين بناءً على نتائج برنامج Amos v22

ملاحظة: تم التأكد من معنوية العلاقات غير المباشرة عن طريق البوتسراب.

تعديلات النموذج النهائي المقترح للدراسة والعلاقات المقترحة

بعد حذف جميع العلاقات غير المعنوية والقيام بالتعديلات المطلوبة توصلنا للنموذج النهائي المعدل والذي يقترحه الباحثان للدراسات اللاحقة من أجل اختباره كما هو موضح في الشكل الموالي:

الشكل رقم: (07): النموذج النهائي المعدل للدراسة



المصدر: من إعداد الباحثين اعتماداً على مخرجات نتائج برنامج Amos v22

V. الخاتمة

في الوقت الذي شهدت فيه وسائل تكنولوجيا المعلومات والاتصال تطوراً مذهلاً واستخداماً بالغ النضير، شرعت الحكومات والدول في عملية الرقمنة لمختلف الهياكل الإدارية من خلال تبنيها لأنظمة الحكومة الإلكترونية، زيادة على

توسيع الاستثمارات في وسائل تكنولوجيا المعلومات والبنية التحتية لقطاع الاتصالات وظهر في مختلف بلدان العالم من خلال التطبيقات المتزايدة لهذه التقنيات، ومن ضمن القطاعات التي استثمرت في هذه التكنولوجيا القطاع المصرفي الذي أصبح يتعامل بمختلف تطبيقاتها ويتعامل عن طريق شبكة الإنترنت محليا ودوليا، والتي أفرزت إلى الوجود نوع جديد من المصارف أصبح يصطلح عليها بالبنوك الإلكترونية التي تعتبر بمثابة تحد جديد أمام المصارف بالنظر للمشاكل التي أصبحت تعترض القطاع المصرفي خاصة تلك المتعلقة بمعلومات وبيانات المستهلكين وخصوصيتهم وحماية وأمن تعاملاتهم الإلكترونية في الفضاء السيبراني والحفاظ على سريتها وسلامتها، لذلك يُعتبر تطوير وسائل الحماية السيبرانية أمر له أهمية بالغة في تفعيل نشاط الصيرفة الإلكترونية، فمن خلال الأمن السيبراني فإن الخدمة المصرفية سوف تتمتع بجميع خصائص جودتها وكذا تُمكن من خلق خدمات أخرى وتولد القيمة وعلى رأسها الخصوصية والسرية والتكنولوجيا المستخدمة والتوافر والديمومة وتتبع الأثر، التي توفر خدمة مصرفية بكافة المقاييس.

كل هذا من شأنه أن يزيد من ثقة المستهلك الإلكتروني بالخدمات المصرفية الإلكترونية لظروف الراحة والأمان التي يشعر بها، ومن هنا نستنتج أن الأمن السيبراني لا يلعب دورا فقط في أمن وجودة الخدمات المصرفية الإلكترونية ولكنه هو أساس وجودة الخدمات المصرفية الإلكترونية التي تحقق رضا المستهلك الإلكتروني.

نتائج الدراسة:

على ضوء الدراسة الميدانية واختبار الفرضيات، قد توصلنا إلى النتائج الآتية:

- من خلال مسار الدراسة تم التأكد من صحة الفرضيات المطروحة في البداية، حيث بعد اختبار الفرضيات الفرعية والتي جاءت كلها تؤكد صدق الفرضية الرئيسية وتشير إلى وجود مساهمة للأمن السيبراني في تحقيق رضا المستهلك الإلكتروني من خلال تعزيز الثقة، وبهذا تكون الدراسة قد أكدت بأن الأمن السيبراني على مستوى البنك هو شرط أساسي لتحقيق رضا المستهلك الإلكتروني المستخدم لبطاقات الدفع الإلكترونية من خلال تعزيز ثقته.
- مستويات أبعاد الأمن السيبراني كانت مرتفعة في عمومها ما عدا بعد سرية البيانات وبعد التوافر والديمومة الذين كانا ضعيفين، يرجع الطالب سبب ذلك إلى حداثة مصطلح الأمن السيبراني من جهة، وعدم الفهم الجيد لأسئلة الاستبانة المخصصة لهاذين البعدين من قبل المستجوبين من جهة أخرى.
- وجود تأثير ذو دلالة إحصائية للأمن السيبراني (احترام الخصوصية، التكنولوجيا المستخدمة، تتبع الأثر) في ثقة المستهلك الإلكتروني لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية BDL بولاية غرداية عند مستوى دلالة 0,05.
- وجود تأثير ذو دلالة إحصائية للثقة في رضا المستهلك الإلكتروني لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية BDL بولاية غرداية عند مستوى دلالة 0,05.
- وجود تأثير ذو دلالة إحصائية للأمن السيبراني (احترام الخصوصية، التكنولوجيا المستخدمة، تتبع الأثر) في رضا المستهلك الإلكتروني من خلال تعزيز الثقة لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية BDL بولاية غرداية عند مستوى دلالة 0,05.

المقترحات:

- خلصت الدراسة إلى اقتراح نموذج معدل لمساهمة الأمن السيبراني في تحقيق رضا المستهلك الإلكتروني من خلال تعزيز الثقة كمتغير وسيطي.
- ضرورة اتخاذ بنك التنمية المحلية تدابير تعتمد على الأمن السيبراني كعنصر ضروري في العملية الإنتاجية للخدمات ومختلف التعاملات الإلكترونية، لا سيما ما يخص البنى التحتية والبرامج والأجهزة المستخدمة في تقنيات المعلومات والاتصال.
- يجب على بنك التنمية المحلية بناء المزيد من الثقة في التعاملات الإلكترونية مع المستهلك الإلكتروني، مع تحديد أسباب ضعف ثقة التعامل ببطاقات الدفع الإلكترونية.
- ضرورة العمل بالنظم المعلوماتية وشبكات الاتصال ذات المواصفات القياسية وتطبيق معايير الجودة الدولية ISO لضمان سلامة أمن المعلومات والبيانات وحمايتها وأمن الشبكات من الاختراقات المحتملة، فضلاً عن أهمية استخدام أنظمة التشغيل ذات المصدر المفتوح (open source software) مثل نظامي الـ Linux و Unix التي تتميز بالاستقرار والأمنية المحكمة.
- ضرورة اتخاذ البنك إجراءات احترازية للحماية والتحصين من أي تخريب أو سطو سيبراني أو أي خطر، والعمل على التحديث المستمر للتقنيات والبرامج المضادة للاعتداءات والفيروسات، بالإضافة إلى اعتماد الوسائل التقنية الحديثة للحماية فيما يخص (التشفير، التصديق الرقمي، البصمة الرقمية، جدار النار، تقنيات أخرى حديثة... الخ).
- ضرورة اعتماد البنك برامج مضادة بالنسخ الأصلية للاستفادة من الدعم الفني للشركات التي يتم شراء البرامج منها.
- ضرورة تأهيل وتكوين كوادر بشرية متخصصة في الأمن السيبراني ومجال الإلكترونيات من أجل أن تقف كحجر عثرة أمام أي محاولة لتهديد أمن البنك عامة وأمن تقديم الخدمات البنكية الإلكترونية خاصة.
- ضرورة الاعتماد على الكفاءات البشرية المحلية في مجال الأمن السيبراني من أجل التحكم في مختلف تقنيات (الأجهزة الإلكترونية، البرمجيات، النظم، الشبكات، الإنترنت،... الخ)، حتى نخرج من التبعية التكنولوجية.
- يجب توعية المستهلكين الإلكترونيين بمختلف الجرائم السيبرانية بما فيها الإحتيال والنصب المالي والمصرفي الإلكتروني وعمليات التعدي والتجسس والتخريب والتدمير وكل ما يتعلق بالتعاملات الإلكترونية ببطاقات الدفع الإلكترونية المصرفية.
- ضرورة قيام الدولة بوضع قوانين وتشريعات شاملة تتماشى مع كل مستجدات الإجرام السيبراني فيما يخص حماية التعاملات الإلكترونية بصفة عامة وحماية البيانات الشخصية للمستهلك الإلكتروني بصفة خاصة في (الفضاء السيبراني) سواء مع البنوك أو غيرها، وتحميل عقوبات مشددة لذلك.

VI. المراجع

1. Cherif-Benmiled, H. (2012). La confiance en Marketing. paris: universite Paris1 Pantheon-Sorbonne.
2. Halliburton, C. (2010). The Role of Trust in Consumer Relationships. ESCP Europe Business School.
3. IUT الاتحاد العالمي للاتصالات (2009). دليل الأمن السيبراني للبلدان النامية. جونيف سويسرا.
4. Ventre, D. (2011). Cyberattaque et cyberdefense. Paris: La Voisier.
5. الجريدة الرسمية ج. ج. (2018, 04-18) القانون رقم 18-04 المتعلق بالقواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، الجزائر.
6. الحازمي، خ. ح. (2006). علاقة السلوك الاستهلاكي للمراهقين ببعض المتغيرات الأسرية. رسالة ماجستير، قسم السكن وإدارة المنزل. السعودية، كلية التربية للاقتصاد المنزلي، جامعة أم القرى، السعودية.
7. العدوان، ع. ص. (2015). أثر جودة الخدمات المصرفية الالكترونية في تعزيز الأداء -دراسة على المصارف التجارية الأردنية. أطروحة دكتوراة. عمان، جامعة العلوم الاسلامية العالمية، الأردن.
8. القحطاني، ب. ب. (2015). أمن المعلومات. لبنان: دار قابس للطباعة والنشر والتوزيع.
9. بوسطة، ع. (2010/2011). أثر التسويق بالعلاقات في تحقيق جودة خدمة العملاء. رسالة ماجستير، علوم تجارية. جامعة الجزائر، الجزائر.
10. جبور، م. أ. (2017). الأمن السايبري تحديات ومستلزمات المواجهة. بيروت، لبنان: دراسات وأبحاث المركز العربي للبحوث القانونية والقضائية (الأمن المعلوماتي والأمن القانوني)
11. شاهين، د. ر. (2013/2014). دور العلامة التجارية في تحقيق رضا المستهلكين. رسالة ماجستير، قسم ادارة الأعمال. سوريا، كلية الاقتصاد الثانية، جامعة تشرين، سوريا.
12. عبد الله، س. م. (2013). أثر ثقة العميل في المؤسسة المصرفية على قبوله التعامل المصرفي عبر الأنترنت. رسالة ماجستير إدارة الأعمال. مصر، كلية التجارة جامعة القاهرة.
13. عطية، ط. أ. (2009). الأمن المعلوماتي. الاسكندرية، مصر: دار الجامعة الجديدة للنشر.
14. فقيه، ت. م. (2013). التسويق الالكتروني وأثره على اتجاهات الأسرة الاستهلاكية في عصر المعلوماتية. رسالة ماجستير قسم السكن وإدارة المنزل، كلية التربية للاقتصاد المنزلي جامعة أم القرى،
15. ياسين، س. غ. (2010). نظم إدارة قواعد البيانات. الأردن، عمان: دار اليازوري العلمية للنشر والتوزيع.