جامعة غرداية – الجزائر
كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير
قسم العلوم التجارية

أطروحة مقدمة لاستكمال متطلبات نيل شهادة دكتوراه أكاديمي – الطور الثالث

في ميدان: العلوم الاقتصادية والعلوم التجارية وعلوم التسيير

شعبة: العلوم التجارية، تخصص تسويق الخدمات

بعنوان:

مساهمة الأمن السيبراني للبيانات في تعزيز ثقة العملاء نحو الخدمات الإلكترونية المصرفية

دراسة ميدانية لدى عينة عملاء بنك التنمية المحلية BDL بولاية غرداية

من إعداد الطالب: عبد القادر صواق

نوقشت وأجيزت علنا بتاريخ: 26 سبتمبر 2024

أمام اللّجنة المكوّنة من السّادة الآتية أسماؤهم:

الاسم واللقب	الرتبة	الجامعة الأصلية	الصفة
حسين شنيني	أستاذ التعليم العالي	جامعة غرداية	رئيسا
بومدين بوداود	أستاذ محاضر أ	جامعة غرداية	مشرفا رئيسيا ومقررا
عبد اللطيف أولاد حيمودة	أستاذ التعليم العالي	جامعة غرداية	مشرفا مساعدا
عبد الحميد مراكشي	أستاذ محاضر أ	جامعة غرداية	مناقشا
عبد الحق بن تفات	أستاذ التعليم العالي	جامعة ورقلة	مناقشا
أحمد بن مويزة	أستاذ التعليم العالي	جامعة الأغواط	مناقشا

السنة الجامعية: 2024-2025


بسم الله الرحمن الرحيم

بسم الله الرحمن الرحيم:

﴿ "ربِّ أوزعني أن أشكر نعمتك التي أنعمت عليَّ وعلى والديَّ وأن أعمل صالحا ترضاه وأدخلني برحمتك في عبادك الصالحين" ﴾ (سورة النمل:19)

أهدي ثمرة جهدي:

إلى أغلى وجود في الدنيا والداي...

إلى أثير الحب والحياة زوجتي وأبنائي...

إلى سندي وعزوتي إخوتي وأصدقائي...

إلى كل أساتذتي بكلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير وأخص بالذكر قسم العلوم التجارية جامعة غرداية.

أشكر الله تعالى وأحمده حمدا كثيرا على تقديره وتوفيقه لإنجاز هذا العمل.

أتقدم بشكري الخالص إلى أساتذتي الدكتور: بومدين بوداود والأستاذ الدكتور: عبد اللطيف أولاد حيمودة على نصائحهما وتوجيهاتهما القيمة وصبرهما على الإشراف.

كما لا يفوتني أن أتوجه بالشكر إلى أعضاء لجنة المناقشة وكل أفراد عائلتي وكافة زملائي في الدراسة وجميع من ساعدني في إنهاء هذا البحث ولو بكلمة طيبة.

ملخص الدراسة

الملخص:

هدفت الدراسة إلى معرفة أبعاد الأمن السيبراني، وتوضيح مدى مساهمتها في تعزيز ثقة العملاء نحو الخدمات الإلكترونية المصرفية لدى عينة من مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية، ومن أجل تحقيق هذه الأهداف تم توزيع الاستبيان لعينة مكونة من (195) مفردة، حيث تم استخدام أسلوب نمذجة المعادلة الهيكلية (SEM) بطريقة المربعات الصغرى الجزئية (PLS) لاختبار الأثر المباشر وغير المباشر لمتغيرات الدراسة واختبار صلاحية وصدق وثبات نموذج الدراسة بالاستعانة بالبرنامج الإحصائي للعلوم الاجتماعية Spss V26 وبرنامج Smart PLS.4.

توصلت الدراسة إلى عدد من النتائج جاء أهمها، وجود تأثير مباشر لأبعاد الأمن السيبراني في ثقة العملاء، حيث تمتع بعدي (سرية البيانات والتكنولوجيا المستخدمة) بأعلى مستوى من التأثير في العلاقة، كما تم تأكيد أن عامل ثقة العملاء من خلال بعديه (الثقة المعرفية، الثقة العاطفية) له أهمية بالغة في الخدمات الإلكترونية المصرفية بتأثير إيجابي كبير، بالإضافة إلى ذلك أثبتت الدراسة وجود تأثير غير مباشر لأبعاد الأمن السيبراني في الخدمات الإلكترونية المصرفية من خلال بعد الثقة المعرفية للعملاء كمتغير وسيط، تمتع فيها كل الأبعاد بأعلى مستوى من التأثير ما عدا بعد (احترام الخصوصية)، وفي الأخير توصلت الدراسة إلى وجود تأثير غير مباشر لأبعاد الأمن السيبراني في الخدمات الإلكترونية المصرفية من خلال بعد الثقة العاطفية للعملاء كمتغير وسيط، تمتع فيها كل الأبعاد بأعلى مستوى من التأثير ما عدا بعدي (التوافر والديمومة، تتبع الأثر)، كانت نتائجهما سلبية.

الكلمات المفتاحية: الأمن السيبراني، البيانات، ثقة العملاء، الخدمات الإلكترونية المصرفية، بطاقات الدفع الإلكتروني.

Abstract:

This study aims to identify the dimensions of cyber security and clarify their contribution to enhancing customer trust in electronic banking services among a sample of electronic payment card users at the Local Development Bank in Ghardaia State, To achieve these objectives, a questionnaire was distributed to a sample of (195) individuals. The Structural Equation Modeling (SEM) method using Squares Path Modeling Partial Least (PLS) was employed to test the direct and indirect effects of the study variables and to test the validity, reliability, and stability of the study model using SPSS V26 and PLS.4 Smart software.

The study reached several findings, the most important of which is the direct impact of cyber security dimensions on customer trust. The dimensions of data confidentiality and the technology used had the highest level of influence in this relationship. It was also confirmed that the factor of customer trust, through its dimensions of cognitive trust and emotional trust, is highly significant in online banking services with a substantial positive effect. Additionally, the study demonstrated an indirect effect of cyber security dimensions on online banking services through customer cognitive trust as a mediating variable, with all dimensions exhibiting a high level of influence except for the dimension of privacy respect. Finally, the study found an indirect effect of cyber security dimensions on online banking services through customer emotional trust as a mediating variable, with all dimensions showing a high level of influence except for the dimensions of availability and continuity, tracking the impact, whose results were negative.

Keywords: Cyber security, Data, Customer Trust, Electronic Banking Services, Electronic Payment Cards

قائمة المحتويات

قائمة المحتويات

قائمة الجداول

قائمة الأشكال

قائمة الملاحق

قائمة المختصرات

الاختصار	الدلالة باللغة الأجنبية	الدلالة باللغة العربية
ADSL	Asymmetric Digital Subscriber Line	الخط المشترك الرقمي غير المتناظر
AEBS	Algeria E-Banking Service	الجزائر لخدمات الصيرفة الإلكترونية
AES	Advanced Encryption Standard	معيار التشفير المتقدم
AFRIPOL	African Criminal Police Organization	المنظمة الافريقية للشرطة الجنائية
AMOS	Analysis of Moment of Structures	التحليل الاحصائي لبنية العزوم
ARCC	Arab Regional Center for Cyber security	المركز العربي الإقليمي للأمن السيبراني
ARTS	Algeria Real Time Settlements	نظام الجزائر للتسوية الفورية
ATCI	Algérie Télé Compensation Interbancaire	المقاصة بين البنوك في الجزائر
ATCI	Algérie Télé Compensation Interbancaire	المقاصة بين البنوك في الجزائر
ATM	Automates Teller Machines	آلات الصرف الذاتي

بنك التنمية المحلية	Banque de Développement Local	**BDL**
رقم ثنائي	Binary Digit	**BIT**
مركز البحث في الإعلام العلمي والتقني	Centre de Recherche sur L'information Scientifique et Technique	**CERIST**
فريق الاستجابة للطوارئ الحاسوب	Computer Emergency Response Team	**CERT**
البطاقات الداخلية البنكية	Carte Inter Bancaire	**CIB**
بنك القرض الشعبي الجزائري	Crédit Populaire d'Algérie	**CPA**
الموزعات الآلية للأوراق النقدية	Distributeurs Automatique de Billets	**DAB**
معيار تشفير البيانات	Data Encryption Standard	**DES**
هجوم تعطيل الخدمة	Denial of Service Attack	**DOS**
الخدمات الإلكترونية المصرفية	Electronic Banking Services	**EBS**
التبادل الإلكترونية للبيانات	Electronic Data Interchange	**EDI**
الشباك الآلي البنكي	Guichet Automatique de Bancaire	**GAB**
بروتوكول نقل النصوص الترابطية	Hypertext Text Transfer Protocol	**HTTP**
آلات الأعمال الدولية	International Business Machines	**IBM**
أجهزة منع الدخلاء	Intrusion Detection System.	**IDS**
المنظمة الدولية للشرطة الجنائية	International Criminal Police Organization	**INTERPOL**
نظام تشغيل الشبكات البينية	Internetworking Operating System	**IOS**
أنظمة كشف التطفل	Intrusion Detection Systems	**IPS**
موجه للخدمات المدمجة	Integrated Services Router	**ISR**
المواصفة القياسية الدولية	International Standard Specifications	**ISO**
مزود خدمة الإنترنت	Internet Service Provider	**ISP**
الاتحاد الدولي للاتصالات	Union Internationale des Télécommunications	**ITU**
شبكة المنطقة المحلية	Local Area Network	**LAN**

سجل الإقلاع الرئيسي	Master Boot Record	**MBR**
التشفير غير المتناظر	Public Key Encryption	**PKE**
طريقة المربعات الصغرى الجزئية	Partial Least Squares Path Modeling	**PLS**
خوارزمية شامير ورافيست	Rivest Shamir Adleman	**RSA**
نظام التسوية الإجمالية الفورية	Real Time Gross Settlement system	**RTGS**
الشبكة المالية بين البنوك	Réseau Monétique Interbancaire	**RMI**
نظام التسوية الإجمالية الفورية	Real Time Gross Settement System	**RTGS**
الشركة الجزائرية لأتمه المعاملات بين البنوك	Société Algérienne d'automatisations des Transaction	**SATIM**
النمذجة بالمعادلات الهيكلية	Structural Equations Modeling	**SEM**
العمليات المالية الآمنة	Secure Electronic Transaction	**SET**
معهد أمن المعلومات	Security Information Institute	**SII**
خدمة الرسائل القصيرة	Short Message Service	**SMS**
الحزمة الإحصائية للعلوم الاجتماعية	Statistical Package for the Social Sciences	**SPSS**
بروتوكول طبقات المنافذ	Secure Sockets Layer	**SSL**
جمعية الاتصالات المالية العالمية بين البنوك	Society for Worldwide Interbank Financial Telecommunications	**SWIFT**
تكنولوجيا الاعلام والاتصال	Technology Information and Communication	**TIC**
أمن طبقة النقل	Transport Layer Security	**TLS**
نهائي الدفع الإلكتروني	Terminal de Paiement Electronique	**TPE**
الولايات المتحدة الأمريكية	United States of American	**USA**
ناقل بيانات شامل	Universal Serial Bus	**USB**
الشبكة الافتراضية الخاصة	Virtual Private Network	**VPN**


مقدمة

توطئة:

يشهد العالم اليوم استخدام واسع للشبكة العالمية للمعلومات في جميع المجالات خاصة التجارية منها، وهو ما فسح المجال للمصارف لتقديم خدماتها بتقنيات جديدة لشريحة عريضة من المتعاملين، ما أدى إلى القفزة النوعية في تحديثها والرفع من قدرتها وجودتها، وتكييفها للاستفادة من المكاسب التي تحققها في مواجهة الآثار السلبية الناجمة عنها، وعليه ظهر مفهوم جديد للصيرفة، ما يسمى بالصيرفة الإلكترونية القائمة على نشاط أكثر تطورا وجاذبية، من خلال تقديم خدمات إلكترونية مصرفية متنوعة في الزمان والمكان المناسبين.

ومن أهم مزايا استفادة المصارف من أحدث تقنيات المعلومات والاتصال، قدرتها على ابتكار خدمات مصرفية مستحدثة مع تطور أساليب تقديمها بما يكفل انسيابها من المصرف إلى العميل، بكل سهولة ويسر ودقة، الأمر الذي يتلاءم مع المتطلبات المعاصرة لمختلف شرائح العملاء من جهة، وتحقيق للمصرف نموا في حجم عملياته وأرباحه من جهة أخرى.

فمسايرة التغيرات والتطورات المذكورة أعلاه لا بد أن يتم وفق آليات وتدابير تحمي الأنظمة والمعلومات المصرفية من جانب، وبيانات وخصوصية العملاء من جانب آخر، نظرا لوجود عدة مخاطر وتهديدات تتعلق بأمن المعاملات الإلكترونية في الفضاء الرقمي وهو ما يطلق عليه بالأمن السيبراني، إذ يُعتبر هذا الأخير أمرا مهما بالنسبة لجميع الأطراف، منها الدول، المؤسسات، وحتى الأفراد، مما يستدعي التفكير مليا في تصميم وإنشاء وإدارة البنيات الأساسية للاتصالات والخدمات والأنشطة التي توفرها بضرورة التركيز على الجانب الأمني، ذلك أن الأمن هو الركن الركين لأي نشاط، وينبغي النظر إليه كخدمة أساسية ذات أولوية تمكن من خلق خدمات أخرى وتتيح القيمة المضافة وميزة تنافسية للمؤسسة، مع الوصول إلى أعلى مستوى من الثقة لدى العملاء.

ولتحقيق عنصر الثقة في عصر الجريمة السيبرانية المتنامية، يجب إرساء قواعد وأنماط من التدابير والإجراءات الأمنية التي تعزز قدرة المؤسسات على حماية بيانات عملائها من مختلف المخاطر والتهديدات، وكقاعدة عامة أنه كلما زادت البيانات أهمية فإنها تتطلب جهودا أكبر في حمايتها لأنها تصبح أكثر عرضة للجرائم السيبرانية وهدف يُراد الوصول إليه من قبل أصحاب النوايا السيئة من خلال الاختراق، السرقة، الاختلاس، التخريب، التهديد، النصب، الابتزاز، تعطيل الخدمة، تدمير البيانات، التلاعب بها، القذف، التشهير، الاعتداء على الملكية الفكرية، إنزال الضرر بالسلع غير الملموسة وبعمليات الإنتاج وحتى صنع القرار وما إلى ذلك، وهذا ما يشهده قطاع الخدمات المالية المصرفية الأكثر القطاعات الاقتصادية تعرضا للمخاطر، إذ يشهد هجمات سيبرانية تفوق القطاعات الأخرى بنسبة 71% وفق تقديرات البنك الدولي، وقد تصل تكلفة تلك الهجمات في قطاع الخدمات المالية إلى ما يقدر بنحو 360 مليار دولار سنويا حال اتساع نطاق انتشارها وفقا لتقارير صندوق النقد الدولي[1]،

[1] محمد اسماعيل، "**الأمن السيبراني في القطاع المصرفي**"، موجز سياسات صندوق النقد العربي، العدد 04، جويلية 2019، ص 1.

الأمر الذي دفع مختلف المصارف العالمية الى تشديد التعليمات الرقابية باتخاذ خطوات وإتباع تدابير واقتناء أدوات لتحسين طريقة إدارة المخاطر السيبرانية.

وفي هذا السياق عملت المصارف الجزائرية على تطوير وسائلها وآلية عملها باعتماد خدمات إلكترونية مصرفية بغية مواكبة مختلف التطورات الحاصلة، والوصول إلى أرقى النظم المعلوماتية المصرفية، عليه قامت تدريجيا بإعادة هيكلة عملياتها من خلال توفير التكنولوجيا الحديثة، البنية التحتية الرقمية، وسائل الحماية، كموارد إستراتيجية فعالة لضمان نموها وبقائها بالاستمرار في التعامل مع عملاءها واستهداف أكبر عدد ممكن، وهذا الأمر لا يتأتى إلا بتعزيز مستوى الثقة لديهم، مع تحقيق أقصى إشباع ممكن بتلبية حاجاتهم ورغباهم المتجددة، وهذا ما دفعنا في دراستنا هذه للبحث عن مدى مساهمة عناصر الأمن السيبراني في تعزيز ثقة العملاء نحو الخدمات الإلكترونية المصرفية في المؤسسة المصرفية الجزائرية.

وانطلاقا من هذا الطرح وفي إطار هاته الدراسة، يُطرح الإشكال المعارفي التالي:

"ما مدى مساهمة أبعاد الأمن السيبراني للبيانات في تعزيز ثقة العملاء نحو الخدمات الإلكترونية المصرفية لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية BDL بولاية غرداية؟

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

1- ما مدى تأثير أبعاد الأمن السيبراني للبيانات في ثقة العملاء لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية؟

2- ما مدى تأثير ثقة العملاء في الخدمات الإلكترونية المصرفية لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية؟

3- ما مدى تأثير أبعاد الأمن السيبراني للبيانات في الخدمات الإلكترونية المصرفية لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية؟

4- ما مدى تأثير أبعاد الأمن السيبراني للبيانات في الخدمات الإلكترونية المصرفية من خلال تعزيز ثقة العملاء لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية؟

فرضيات الدراسة:

للإجابة على التساؤلات المطروحة سابقا فإننا نستعين بفرضيات الدراسة التالية:

–هناك تأثير مباشر لأبعاد الأمن السيبراني للبيانات في تعزيز ثقة العملاء لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.

–هناك تأثير مباشر لثقة العملاء في الخدمات الإلكترونية المصرفية لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.

–هناك تأثير مباشر لأبعاد الأمن السيبراني للبيانات في الخدمات الإلكترونية المصرفية لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.

–هناك تأثير غير مباشر لأبعاد الأمن السيبراني للبيانات في الخدمات الإلكترونية المصرفية من خلال تعزيز ثقة العملاء لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.

أهداف الدراسة:

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

– تقييم مدى تأثير أبعاد الأمن السيبراني على ثقة العملاء نحو استخدام الخدمات الإلكترونية المصرفية.

–معرفة طبيعة العلاقة المباشرة وغير المباشرة بين أبعاد الأمن السيبراني للبيانات وتأثيرها على ثقة العملاء نحو الخدمات الإلكترونية المصرفية.

– بناء نموذج نظري للعلاقات السببية بين متغيرات الأمن السيبراني وثقة العملاء في استخدام الخدمات الإلكترونية المصرفية.

– اختبار العلاقة السببية بين متغيرات الدراسة لفهم وتحليل مسارات العلاقات المتداخلة والمتكاملة المباشرة وغير المباشرة.

–تسليط الضوء على واقع استخدام عملاء البنك للخدمات الإلكترونية المصرفية ومدى ثقتهم بها.

– تزويد متخذي القرار في المنظومة المصرفية بأهمية وفعالية اعتماد الأمن السيبراني بأبعاده (احترام الخصوصية، سرية البيانات، التوافر والديمومة، التكنولوجيا المستخدمة، تتبع الأثر)، بما يعزز ثقة العملاء نحو الخدمات الإلكترونية المصرفية.

أهمية الدراسة:

أشارت الكثير من الباحثين إلى أن هناك حراك كبير في العالم أجمع نحو أمن المعلومات والشبكات والأمن السيبراني، إذ يستمد البحث الحالي أهميته العلمية كونه من البحوث التي تهتم بالتعرف على الأمن السيبراني للبيانات في القطاع المصرفي كأحد الموضوعات الحديثة والمتطورة باستمرار بسبب تزايد المخاطر والتهديدات السيبرانية العابرة للحدود التي تهدد استمرارية المؤسسات وأدائها، لذلك يجب التعرف على مدى مساهمة الأمن السيبراني في تعزيز ثقة العملاء نحو الخدمات الإلكترونية المصرفية، ويكتسي الموضوع أهمية بالغة نظرا لما يلي:

- أهمية قطاع البنوك في الوقت الراهن، حيث تمثل البنوك المحرك الأول لعمليات تمويل التنمية وبالتالي فإن دراسة الأمن السيبراني للبنوك له أهمية كبيرة.
- يشهد سوق العمل حاجة مستمرة لخبراء في مجال الأمن السيبراني.

- عدم وجود دراسات ميدانية كافية اهتمت بالأمن السيبراني في البنوك التجارية الجزائرية وقياس مدى مساهمته في الرفع من مستوى ثقة العملاء نحو الخدمات الإلكترونية المصرفية.
- 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.
- تقدم الدراسة إطار أكاديمي يُثري المكتبة الجزائرية بموضوعات تزداد أهميتها في ظل التطورات التكنولوجية وظهور التقنيات المختلفة والمخاوف السيبرانية لدى الكثير من الفئات.
- تقدم الدراسة نتائج وتوصيات تثري معارف العملاء ومستخدمي البنوك والأكاديميين والمؤسسات الرقمية حول الأمن السيبراني والثقافة الرقمية وطرق حماية البيانات وآليات تعزيز الثقة نحوها.
- قد تفيد نتائج الدراسة الحالية الباحثين والمختصين، حيث تفتح لهم آفاقا لدراسات مستقبلية تتعلق بالأمن السيبراني والثقة الرقمية وتطبيقاتها في القطاعات الأخرى.

مبررات اختيار الدراسة:

➢ مبررات ذاتية:

- الرغبة الشخصية للطالب لمثل هاته المواضيع، مع انتمائه للمؤسسة الأمنية.
- وجود مكتب خاص بمكافحة الجرائم السيبرانية بأمن ولاية غرداية.

➢ مبررات موضوعية:

- تماشي الموضوع مع طبيعة التخصص (تسويق الخدمات)، فتوفير عنصر الأمن السيبراني للخدمات الإلكترونية على مستوى البنوك يعتبر الركن الركين لنشاط تعاملاته الإلكترونية، ومن بين الخدمات الأساسية التي من خلالها تمكن من خلق خدمات أخرى وتولد القيمة، بالإضافة إلى أن الخدمة الإلكترونية المصرفية سوف تتمتع بجميع خصائص جودتها.
- وجود المشاكل والجرائم السيبرانية خاصة استهداف المجرمين للقطاع المالي.
- مدى أهمية ثقة العملاء في التعاملات الإلكترونية بالنسبة للمؤسسات التجارية عامة والمصرفية خاصة.
- تزايد التبادل الإلكتروني، إذ يعيش العالم نموا ملحوظا في استخدام الخدمات الإلكترونية المصرفية والتبادلات المالية عبر الإنترنت، مما يزيد من أهمية دراسة عنصر الأمن السيبراني لها.
- تزايد التهديدات السيبرانية وخطورتها بسبب حالات الاختراق والهجمات السيبرانية على مختلف المؤسسات المقدمة للخدمات الإلكترونية قصد تعطيلها، أو سرقة البيانات أو تخريبها، خاصة منها المصارف.
- تم اختيار الدراسة ببنك، نظرا لكونه من أهم المؤسسات المالية التي يعتمد عليها اقتصاد الدولة، بمعنى حساسية القطاع، إضافة إلى أن البنوك في الجزائر هي حديثة الرقمنة والتعاملات الإلكترونية المحلية والدولية باستخدام

شبكة الإنترنت واستعمال البطاقات الإلكترونية المختلفة، بذلك هي بحاجة ماسة لمثل هاته الدراسات، وبالضبط تم اختيار بنك التنمية المحلية غرداية، أولا: كونه وكالة وفي نفس الوقت مديرية جهوية، ثانيا: لاحتوائه على خلية تقنية تابعة لدائرة الإدارة تتمثل في خلية الإعلام الآلي، التي تفيدنا بالمعلومات حول عناصر الحماية التقنية والإجراءات والتدابير الأمنية السيبرانية للمعاملات المالية الرقمية.

- تعتبر هذه الدراسة تكملة لمذكرة الماستر الخاصة بالطالب، والتي كان عنوانها: "مساهمة الأمن السيبراني للبيانات في تحقيق رضا المستهلك الإلكتروني"، محاولا بذلك المواصلة في نفس مسار الدراسة والتعمق فيها أكثر.

حدود الدراسة:

- **الحدود المكانية:** تم إجراء البحث على عينة من مستخدمي الخدمات الإلكترونية المصرفية من خلال بطاقات الدفع الإلكترونية بمختلف أنواعها على مستوى بنك التنمية المحلية وكالة ولاية غرداية.
- **الحدود البشرية:** تم اختبار عينة عشوائية ميسرة مكونة من (195) من مستخدمي الخدمات الإلكترونية المصرفية من خلال بطاقات الدفع الإلكترونية على مستوى بنك التنمية المحلية وكالة ولاية غرداية.
- **الحدود الزمنية:** بالنسبة للجانب التطبيقي كان خلال الفترة الممتدة من: 2024/02/01 إلى 2024/05/11 مقسمة بين توزيع وجمع الاستبيانات وتحليلها.
- **الحدود الإجرائية:**
  - بالنسبة لمتغيرات الدراسة فالمتغير المستقل هو "الأمن السيبراني"، إذ نقصد به النشاط أو الخدمة التي تُؤمَن وتحمي الموارد المرتبطة بتقنية المعلومات والاتصال الخاصة بالبنك من أي مخاطر أو اعتداءات في الفضاء السيبراني بغية عدم توقف المنشأة عن العملية الإنتاجية مهما كان الوضع، من خلال الأبعاد الخمسة: سرية البيانات، التوافر والديمومة، تتبع الأثر، احترام الخصوصية، التكنولوجيا المستخدمة، وهذا ما هو متوفر في البنك محل الدراسة الأمر الذي يسهل علينا الدراسة الميدانية.
  - أما المتغير الوسيط "ثقة العملاء"، نقصد بها توقعات العملاء مع إرادتهم الفعلية للاعتماد على البنك محل الدراسة دون غيره في تحقيق نتائج مرغوبة، واستعدادهم لقبول درجة الخطر، إذ يسهم تعزيزها في كسب ودهم وجذبهم من أجل استخدام الخدمات الإلكترونية المصرفية.
  - بالنسبة للخدمات الإلكترونية المصرفية، فهي مختلف المنتجات والخدمات المصرفية المقدمة إلكترونيا إلى العملاء أينما كانوا، وقد تكون خدمات عبر الإنترنت، خدمات افتراضية وغيرها.

منهج البحث والأدوات المستخدمة في الدراسة:

لدراسة موضوع البحث، تم الاعتماد على المنهج الوصفي التحليلي ما يناسب تقرير الحقائق والتعريف بمختلف المفاهيم ذات الصلة بالموضوع، حيث اعتمدنا على أسلوب النمذجة بالمعادلات الهيكلية (SEM) (Structural Equations Modeling) بطريقة المربعات الصغرى الجزئية (PLS) Partial Squares Path Modeling Least وذلك من أجل الحصول نتائج أكثر دقة، وهو يعد من بين أفضل الطرق الحديثة التي تستخدم لاختبار النماذج متعددة المتغيرات خاصة في ظل وجود المتغير الوسيطي، مما يستدعي دراسة العلاقات بين المتغيرات جميعا من خلال قياس التأثير المباشر وغير المباشر بين المتغير المستقل الأمن السيبراني على المتغير التابع الخدمات الإلكترونية المصرفية بوجود ثقة العملاء كمتغير وسيط، وهذا باستخدام أساليب إحصائية عن طريق برنامج Spss v26 و Smart PLS.4.

الدراسات السابقة باللغة العربية:

سنتناول في هذا المبحث بعض الدراسات السابقة باللغة العربية التي لها علاقة بموضوع الدراسة، كما يلي:

01-دراسة: عمرو أحمد نور الدين، (2022)، بعنوان: "أثر المخاطر المدركة على استخدام الخدمات المصرفية الإلكترونية في مصر: الدور الوسيط لتوقعات الثقة -دراسة ميدانية".[1]

هدفت الدراسة إلى التعرف على الدور الوسيط لتوقعات الثقة في العلاقة بين المخاطر المدركة واستخدام الخدمات المصرفية الإلكترونية في مصر، وقد اعتمد الباحث على المنهج الوصفي من خلال إجراء البحث على عينة مكونة من (384) مفردة، وتم جمع البيانات بواسطة الاستقصاء حيث بلغ عدد الاستمارات الصالحة للتحليل الإحصائي (314) استمارة بنسبة استجابة قدرها (81،77%)، وتم تحليل البيانات بواسطة نموذج المعادلات الهيكلية (SEM) باستخدام برنامج AMOS. V25.

توصلت الدراسة إلى عدة نتائج جاء أهمها إلى وجود تأثير معنوي إيجابي لتوقعات الثقة على استخدام الخدمات المصرفية الإلكترونية عندما ترتفع توقعات الثقة يرتفع استخدام الخدمات المصرفية الإلكترونية، كما تبين أن التأثير المباشر (غير الوسيط) هو تأثير معنوي سلبي للمخاطر المدركة من العميل على استخدام الخدمات المصرفية الإلكترونية أي عندما ترتفع المخاطر المدركة ينخفض استخدام الخدمات المصرفية الإلكترونية، أما على مستوى التأثير غير المباشر فقد تبين أن توقعات الثقة تتوسط بشكل جزئي في تأثير المخاطر المدركة على استخدام الخدمات المصرفية الإلكترونية، حيث أن وجود توقعات الثقة يخفض من تأثير المخاطر المدركة على استخدام الخدمات المصرفية الإلكترونية والعكس صحيح.

02-دراسة: يبدري ربيعة (2022)، بعنوان: "دور الأمن السيبراني في حماية المعاملات المالية المصرفية".[2]

هدفت الدراسة إلى التعرف على مدى فعالية دور الأمن السيبراني في حماية المعاملات المالية المصرفية الإلكترونية المبرمة في الشكل الإلكتروني، حيث اعتمد الباحث على المنهج الوصفي التحليلي بغية الإحاطة بالموضوع وتحليل كافة المفاهيم والجوانب المحيطة به من خلال دراسة النصوص القانونية ذات الصلة بالأمن السيبراني للمنظومة المصرفية بالجزائر.

توصلت الدراسة إلى عدة نتائج جاء أهمها أن مجال الأمن السيبراني لا ينحصر داخل الحدود الجغرافية للدول، بل هو يشمل كافة الدول بغض النظر عن الحدود الترابية التي تفصل كل دولة عن نظيرتها، بالإضافة إلى التأكيد على أن الأمن السيبراني وسيلة أثبتت فعاليتها في حماية الأنظمة الرقمية من الهجمات الفيروسية الإلكترونية لقواعد البيانات الحساسة.

---

[1] عمرو أحمد نور الدين، "**أثر المخاطر المدركة على استخدام الخدمات المصرفية الإلكترونية في مصر: الدور الوسيط لتوقعات الثقة -دراسة ميدانية**"، مجلة جامعة الإسكندرية للعلوم الإدارية، كلية التجارة، جامعة الإسكندرية مصر، المجلد 59، العدد 3، 2022، ص ص141-178.

[2] يبدري ربيعة، "**دور الأمن السيبراني في حماية المعاملات المالية المصرفية**"، مقال منشور في كتاب أعمال المؤتمر الدولي العلمي استخدام التكنولوجيا في المؤسسات المالية والمؤسسات الناشئة، إصدار المركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية، برلين، ألمانيا، 04 -05-جوان 2022، ص ص 463-472.

03-دراسة: منير عبد الله مفلح البيشي (2021)، بعنوان: "الأمن السيبراني في الجامعات السعودية وأثره في تعزيز الثقة الرقمية من وجهة نظر أعضاء هيئة التدريس: دراسة على جامعة بيشة".[1]

هدفت الدراسة إلى معرفة واقع الأمن السيبراني في الجامعات السعودية وأثره في تعزيز الثقة الرقمية من وجهة نظر أعضاء هيئة التدريس، ولتحقيق أهداف الدراسة أستخدم المنهج الوصفي التحليلي، وكانت أداة الدراسة عبارة عن الاستبانة وزعت على عينة اختيرت عشوائيا بلغت 182 عضو هيئة تدريس، كما اعتمد الباحث في التحليل على استخدام البرنامج الإحصائي للعلوم الاجتماعية SPSS V22.

توصلت الدراسة إلى عدة نتائج جاء أهمها أن واقع الأمن السيبراني بالجامعات السعودية من وجهة نظر أعضاء هيئة التدريس مرتفعا بنسبة (73،18%)، كما تبين أن مستوى الثقة الرقمية للجامعات السعودية من وجهة نظر أعضاء هيئة التدريس مرتفعا بنسبة (74،58%)، وتبين أن الأمن السيبراني في الجامعات السعودية يؤثر في تعزيز الثقة الرقمية حيث بلغت نسبة التأثير (46،70%)، وتبين أنه لا توجد فروق بين استجابات المبحوثين حول الأمن السيبراني في الجامعات السعودية وأثره في تعزيز الثقة الرقمية تعزى لمتغيري سنوات الخدمة والدرجة العلمية والتفاعل بينهما.

04-دراسة: بن صالح ماجدة (2021)، بعنوان: **"العوامل المؤثرة على ثقة العملاء في الخدمات المصرفية الإلكترونية".**[2]

هدفت الدراسة إلى التعرف على مجموعة العوامل المؤثرة على ثقة العملاء في الخدمات المصرفية الإلكترونية في الجزائر، مفترضة أن كل من: خصائص الخدمة، الأمان، السرية، سهولة الاستخدام، وخصائص البنك المتمثلة في سمعته وحجمه، وخصائص المستهلك المتمثلة في التجارب السابقة والكفاءة في استخدام الحاسب الآلي هي متغيرات مستقلة تؤثر على الثقة في الخدمات المصرفية الإلكترونية كمتغير تابع في أنموذج الدراسة، فكانت الدراسة الميدانية على عينة مقصودة من عملاء بعض البنوك في الجزائر بلغ عددها: 154 مفردة من خلال توزيع الاستبانة عليهم، كما اتبعت الباحثة المنهج الكمي من خلال تحويل البيانات التي تم تجميعها إلى أرقام، وتحليلها باستخدام البرنامج الإحصائي AMOS وSPSS بالإضافة إلى الاعتماد على المقابلات لدعم تفسير النتائج.

توصلت الدراسة إلى مجموعة من النتائج أبرزها: ثبوت كافة العوامل المقترحة، أن من أهم مقومات بناء الثقة في الخدمات المصرفية الإلكترونية هي الأمان والسرية والتي لا زالت تشكل معضلة كبرى حتى على الدول العظمى التي تحتل المراتب الأولى في المجال البنكي ورغم تشديد الإجراءات الأمنية والرقابية على مختلف المخاطر البنكية الناجمة عن التعاملات المصرفية الإلكترونية، أما سهولة الاستخدام المدركة والتجارب السابقة للعميل

---

[1] منير عبد الله مفلح البيشي، **"الأمن السيبراني في الجامعات السعودية وأثره في تعزيز الثقة الرقمية من وجهة نظر أعضاء هيئة التدريس: دراسة على جامعة بيشة"**، مجلة الجامعة الإسلامية للدراسات التربوية والنفسية، جامعة المملكة العربية السعودية، المجلد 29، العدد 6، 2021، ص ص353-372.

[2] بن صالح ماجدة، **"العوامل المؤثرة على ثقة العملاء في الخدمات المصرفية الإلكترونية – دراسة حالة البنوك الجزائرية"**، أطروحة دكتوراه، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، قسم علوم التسيير، شعبة علوم التسيير، جامعة 8 ماي 1945 ولاية قالمة، الجزائر، 2021.

المصرفي وكفاءته في استخدام الحاسب الآلي فهي عوامل يمكن التحكم فيها بتسهيل الإجراءات وتعريب المواقع وتبسيط المراحل اللازمة لتنفيذ العمليات المصرفية الإلكترونية، وبالنسبة لحجم وسمعة البنك المدركة فهما عاملان مهمان جدا لبناء الثقة في البنك أولا ثم الخدمات المقدمة سواء تقليدية أو إلكترونية.

05-دراسة: مروة فتحي البغدادي (2021)، بعنوان: "اقتصاديات الأمن السيبراني في القطاع المصرفي"[1]

تناولت هاته الدراسة أهم التحديات التي تواجه القطاع المالي وبشكل خاص المصرفي في دولة مصر، من أجل تحقيق الأمن السيبراني، والذي يلعب دورا محوريا في معالجة التحديات المستقبلية نظرا لاستخدامه كتكنولوجيا لإدارة الشبكات، الأمر الذي يساعد في تحقيق عدد من أهداف التنمية المستدامة: كتحسين إدارة استخدام المعدات وصيانتها، زيادة الإنتاج، توسيع نطاق الوصول إلى المعلومات المتعلقة بالتفاعل الاقتصادي بين المؤسسات الخاصة والعامة، ولتحقيق أهداف الدراسة أستخدم المنهج التحليلي والمقارن.

توصلت الدراسة إلى عدة نتائج أهمها أن الطبيعة المتطورة للمخاطر السيبرانية ليست قابلة للتنظيم بشكل محدد، كما أن القضايا الخاصة بالإنترنت (Cyber Issues) يمكن معالجتها من خلال اللوائح الحالية المتعلقة بكل من المخاطر التشغيلية والتقنيات، إضافة إلى أن التطور الحادث في المخاطر السيبرانية يحفز المؤسسات المالية على البحث المستمر والمكثف نحو اتخاذ إجراءات وقائية من تلك المخاطر الأمر الذي يؤدي غلى خلق حافز أكبر على الاستثمار بشكل مستمر في تحسين الأمن السيبراني.

06-دراسة: حسن نجيب الرواش، وآخرون (2020)، بعنوان: "محددات استخدام الخدمات الإلكترونية المصرفية في الأردن من وجهة نظر العملاء".[2]

هدفت الدراسة إلى التعرف إلى الأسباب التي تحد من استخدام الخدمات المصرفية عبر الإنترنت في الأردن، ومعرفة الخصائص الديموغرافية في مجال استخدامها، وهذا من خلال تحليل خمسة متغيرات هي: (الأمن والخصوصية، الثقة، سهولة الاستخدام، الفائدة المتوقعة، الاحتياجات البنكية)، ولتحقيق أهداف الدراسة أستخدم المنهج الوصفي التحليلي، وكانت أداة الدراسة عبارة عن الاستبانة، حيث وزعت على عينة احتمالية عشوائية بسيطة بلغت 302 من عملاء البنوك العاملين في الجامعات الخاصة (موظفين بالجامعات) بإقليم الشمال في الأردن كون هاته الجامعات في التوظيف تشترط أن يكون لكل موظف حسابا بنكيا، كما اعتمد الباحث في التحليل على استخدام البرنامج الإحصائي للعلوم الاجتماعية SPSS.

---

[1] مروة فتحي البغدادي، "**اقتصاديات الأمن السيبراني في القطاع المصرفي**"، مجلة البحوث القانونية والاقتصادية، مدرسة الاقتصاد والمالية العامة بالمعهد المصري، أكاديمية الإسكندرية للإدارة والمحاسبة، الجامعة المصرية، الإسكندرية، مصر، المجلد 11، العدد 2، الرقم المسلسل للعدد 76، 2021، ص ص 1446-1516.

[2] حسن نجيب الرواش، رعد مشعل محمد التل، صالح إبراهيم العمر، "**محددات استخدام الخدمات المصرفية الإلكترونية في الأردن من وجهة نظر العملاء**"، المجلة العالمية للاقتصاد والأعمال الأردن، المجلد 08، العدد 03، 2020، ص 375-391. الموقع: https://doi.org/10.31559/GJEB2020.8.3.3، تاريخ الاطلاع: 11-03-2022، الساعة: 22:30.

توصلت الدراسة إلى عدة نتائج جاء أهمها عدم وجود فروقات ذات دلالة إحصائية على جميع مجالات الدراسة تبعا لمتغير الجنس، ووجود فروقات ذات دلال إحصائية لمجال الاحتياجات البنكية والمرحلة العمرية لخمسين سنة فأكثر، ووجود دلال إحصائية لمجال الفائدة المتوقعة والتحصيل العلمي دراسات عاليا.

07-دراسة: الزهرة برة وجميلة حميدة (2019)، بعنوان: "شهادة التصديق الإلكتروني كآلية لتعزيز الثقة في المعاملات الإلكترونية".[1]

هدفت الدراسة إلى معرفة شهادة التصديق الالكتروني وتوضيح دورها في توثيق المعاملات الإلكترونية بصفة عامة والتجارة الإلكترونية بصفة خاصة لاسيما عبر شبكة الإنترنت وهذا من خلال تعزيز عنصر الثقة والأمان، ولتحقيق أهداف الدراسة أتبع المنهج الوصفي من خلال الكشف عن الإطار المفاهيمي المتعلق بالمتغيرات ومراجعة بعض الأدبيات ووصف طبيعة العلاقة بين المتغيرات والخروج باستنتاجات.

توصلت الدراسة إلى أن شهادة التصديق الإلكتروني تتمتع بقيمة قانونية وحجية كاملة في الإثبات شأنها شأن المحررات الرسمية وتعد دليلا تقنيا يعول عليه في الإثبات إذا ما توفرت فيها مجموعة من الشرط التي نص عليها القانون، في مقدمتها صدورها من جهة مختصة مرخص لها أو معتمدة، احتوائها على مجموعة من البيانات واستجابتها لمقتضيات الثقة والأمان.

08-دراسة: محمد الشرفي وآخرون، (2018)، بعنوان: " تأثير ثقة العملاء وتصورهم للأمن والخصوصية على قبول الخدمات المصرفية عبر الإنترنت".[2]

هدفت الدراسة إلى التحقيق في تأثير تصورات الأمن والخصوصية للعملاء على قبولهم اعتماد الخدمات الإلكترونية المصرفية بدولة الأردن، حيث ركزت الدراسة في العوامل التي تؤثر علا ثقة العملاء في قبول استخدام الخدمات المصرفية عبر الإنترنت، وقد اعتمد الباحثون على نموذج دراسة يدعم النموذج النظري TAM مطور يعكس بدقة العوامل التي تؤثر على ثقة العملاء في قبول واستخدام الخدمات الإلكترونية المصرفية. كما اعتمد الباحثون على المنهج الوصفي من خلال إجراء البحث على عينة مكونة من (198) مفردة، وتم جمع البيانات بواسطة استمارات الاستبيان، وتم تحليل البيانات بواسطة نمذجة المعادلة الهيكلية (SEM) باستخدام برنامج AMOS. V21.

توصلت الدراسة إلى عدة نتائج جاء أهمها أن للثقة أثر إيجابي على نية العملاء السلوكية لاعتماد الخدمات المصرفية عبر الإنترنت، علاوة على ذلك تصور العملاء لفائدتهم وأمن خصوصيتهم كان له أيضا تأثير كبير على ثقتهم، ومع ذلك فإن سهولة الاستخدام المتصورة للمستخدمين فشلت في ذلك.

---

[1] الزهرة برة وجميلة حميدة، **"شهادة التصديق الإلكتروني كآلية لتعزيز الثقة في المعاملات الإلكترونية"**، مجلة العلوم القانونية والسياسية، جامعة لونيسي علي العفرون، البليدة 2، الجزائر، المجلد 10، العدد 01، 2019، ص ص 892-911.

[2] محمد الشرفي، رزيني عبد الله، فادي حرز الله، عماد أبو شنب، **"تأثير ثقة العملاء وتصورهم للأمن والخصوصية عند قبول الخدمات المصرفية عبر الانترنت"**، مجلة الإدارة الصناعية، جامعة ماليزيا، المجلد 04 جوان 2018، ص ص 2289-2316.

09-دراسة: عبد الله سيد ماهر بدوي، (2013)، بعنوان: "أثر ثقة العميل في المؤسسة المصرفية على قبوله التعامل المصرفي عبر الإنترنت".[1]

هدفت الدراسة إلى قياس ثقة عملاء البنك على قبولهم التعامل المصرفي عبر الإنترنت، حيث اعتمد البحث على سؤالين بحثيين يتعلقان بالثقة كمفهوم متعدد الأبعاد يشمل ثلاثة أبعاد رئيسية (الأمانة، القدرة، النفع) تعمل كمؤشرات antécédents للثقة العامة (في البنك كمؤسسة، في الخدمة كمنتج، في الإنترنت كوسيط)، هذه الثقة تعتبر مؤشرا مباشرا لكل من الاتجاه نحو الاستخدام والنية السلوكية لاستخدام التعامل المصرفي عبر الإنترنت، اتبع الباحث المنهج المختلط (الوصفي، الكمي) لما فيه من تحسين وتدعيم الثقة في النتائج، كما تبنى مدخل البحث السببي أو التفسيري بهدف توضيح الظاهرة وتفسيرها في شكل علاقات سببية، كما تمت الدراسة من خلال استبانة وزعت على عينة بلغ عددها 290 فرد من عملاء البنوك التجارية بالقاهرة بدولة مصر، في حين استخدمت الدراسة أسلوب نمذجة المعادلة الهيكلية Structure Equation Modeling (SEM) لاختبار صلاحية وصدق وثبات نماذج القياس، وتفسير الآثار المباشرة وغير المباشرة بين متغيرات البحث وتتبع العلاقة السببية بينها، باستخدام برنامج تحليل الهيكلة اللحظية Amos V21..

أوضحت نتائج الدراسة أن الثقة مفهوم متعدد الأبعاد (الأمانة، القدرة، النفع) تعمل كمؤشرات للثقة العامة في التعامل المصرفي عبر الإنترنت (البنك، الخدمة، الإنترنت) وتفسر 43% منها، كما تعتبر أحد أهم مؤشرات قبول التعامل المصرفي عبر الإنترنت، ولها تأثير معنوي مباشر على النية السلوكية لاستخدام التعامل المصرفي عبر الإنترنت. وأن النفع المدرك للبنك على الإنترنت هو أهم عوامل الثقة في التعامل المصرفي عبر الإنترنت، يليه الأمانة المدركة ثم القدرة المدركة للبنك عبر الإنترنت.

10-دراسة: محمد عصمان، شريف مهدي (2011)، بعنوان: "الثقة والأمان في الخدمات المصرفية الإلكترونية في البنوك التجارية السعودية: آراء السعوديين مقابل غير السعوديين".[2]

هدفت الدراسة إلى فحص ثقة وأمن الخدمات المصرفية الإلكترونية في البنوك التجارية السعودية، مع اجراء مقارنة لآراء العملاء السعوديين وغير السعوديين، فكانت الدراسة الميدانية على عينة عشوائية من عملاء مجموعة بنوك بالسعودية في أربعة مدن في المنطقة الشرقية للمملكة العربية السعودية، بلغ عددها: 418 مفردة بمعدل استجابة بلغ: 76.4%، من خلال توزيع الاستبانة عليهم، كما اتبع الباحثين المنهج الوصفي، عن طريق جمع البيانات واستخدام تقنية كرة الثلج (التكاثر)، مع تحليل البيانات على أساس النهج الكمي باستعمال البرنامج الإحصائي SPSS.

---

[1] عبد الله سيد ماهر بدوي، **"أثر ثقة العميل في المؤسسة المصرفية على قبوله التعامل المصرفي عبر الإنترنت"** رسالة ماجستير في إدارة الأعمال، كلية التجارة، قسم إدارة الأعمال، جامعة القاهرة، مصر، 2013.

[2] محمد عصمان، شريف مهدي، **"الثقة والأمان في الخدمات المصرفية الإلكترونية في البنوك التجارية السعودية: آراء السعوديين مقابل غير السعوديين"**، مجلة إدارة الأعمال، المجلد 5، العدد 14، 2011، ص ص 5524-5535.

توصلت الدراسة إلى مجموعة من النتائج أبرزها: وجود فروق ثقة كبيرة بين السعوديين وغير السعوديين في استخدام الخدمات المصرفية الإلكترونية، بما في ذلك أجهزة الصراف الآلي وبطاقات الائتمان والرسائل المصرفية النصية القصيرة عبر الهاتف والخدمات المصرفية الأخرى عبر الإنترنت، كما كشفت النتائج عن مدى ثقة عملاء البنوك السعودية بدرجة كبيرة باستخدام الخدمات المصرفية الإلكترونية مع اعتقادهم بقوة أنها أكثر أمانا مقارنة بنظيراتها من غير السعوديين، كما قدمت الدراسة أدلة تجريبية جديدة تعزز فهمنا للثقة والأمان لتكنولوجيا الخدمات المصرفية الإلكترونية في البنوك الإلكترونية السعودية.

الدراسات السابقة باللغة الأجنبية:

سنتناول في هذا المبحث بعض الدراسات السابقة باللغة الأجنبية التي لها علاقة بموضوع الدراسة، وهي كما يلي:

01-دراسة: Khalid Khalil، (2021)، بعنوان:

"Cyber Security in Electronic Banking and its Impact Upon Electronic Banking".

" الأمن السيبراني في الأعمال المصرفية الإلكترونية وتأثيره على الخدمات الإلكترونية المصرفية".[1]

هدفت الدراسة إلى قياس العلاقة السببية لتكاليف الأمن السيبراني من خلال المتغيرات التالية: المنع/الكشف، الاستجابة، التطوير، الصيانة، على الأداء المالي للخدمات الإلكترونية المصرفية، وكذا فحص تأثير أداء ابتكار المنتج على الأداء المالي للخدمات الإلكترونية المصرفية، وكذا إيجاد متغير وسيط في علاقة تأثير أداء ابتكار المنتجات على تكاليف الأمن السيبراني وأداء الخدمات الإلكترونية المصرفية، ولتحقيق أهداف الدراسة أستخدم المنهج الوصفي التحليلي، وكانت أداة الدراسة عبارة عن الاستبانة وزعت على عينة مستهدفة من كوادر الإدارة وموظفي ثمانية (08) بنوك إلكترونية المتنوعة موجودة في كل من خيبر وإسلام أباد ومدن البنجاب الباكستانية، حيث بلغت 550 مفردة بنسبة استرجاع 98%، كما اعتمد الباحث في التحليل على استخدام نمذجة المعادلة الهيكلية SEM بالبرنامج الإحصائي للعلوم الاجتماعية SPSS وبرنامج AMOS.

توصلت الدراسة إلى عدة نتائج جاء أهمها أن تكاليف الأمن السيبراني لها تأثير إيجابي كبير على الأداء المالي لابتكار المنتجات والخدمات الإلكترونية المصرفية، كما أن لابتكار المنتج تأثير إيجابي كبيرة على الأداء المالي للخدمات الإلكترونية المصرفية، بالإضافة إلى أداء ابتكار المنتج توسط جزئيا العلاقة بين تكاليف الأمن السيبراني وأداء التمويل المصرفي الإلكتروني، ومن هنا كان لتكاليف تأمين تكنولوجيا المعلومات (تكاليف الكشف

[1] Khalid Khalil, **"Cyber Security in Electronic Banking and its Impact Upon Electronic Banking",**Thesis is to Business Administration Department of IQRA National University, Peshawar, Khyber Pakhtunkhawa, Pakistan In Partial Fulfillment of the Requirements for the degree of Doctor of Philosophy in Management Sciences Business", 2021. Https://prr.hec.gov.pk/jspui/bitstream/23456789/17574/1/khalid%khalil, Retrieved: 16-03-2022, 22:10.

والمنع) تأثير كبير على إنتاج المنتجات الإلكترونية المصرفية، أما المنتجات والخدمات فكان لها تأثير إيجابي على عمليات البنوك اليومية.

02-دراسة: Ibrahim Maimunatu، Umar Muazu، (2021)، بعنوان:

"Security and Privacy Dimension as Predictor of Internet Banking E-Service Quality on Customer Trust"

"بعد الأمن والخصوصية كمؤشر لجودة الخدمات الإلكترونية المصرفية عبر الإنترنت على ثقة العملاء"[1]

هدفت الدراسة إلى تأكيد أن بعد الأمن والخصوصية كمؤشر لجودة الخدمات الإلكترونية المصرفية عبر الإنترنت على ثقة العملاء، ولعبها دورا رئيسيا في تحسين جود الخدمات وتحسين العملية المتعلقة بالصناعة المصرفية، ولتحقيق أهداف الدراسة أستخدم المنهج الوصفي التحليلي مع فحص جودة ثقة العملاء باستخدام النموذج E-S-QUAL، وكانت أداة الدراسة عبارة عن الاستبانة وزعت على عينة اختيرت عشوائيا بلغت 379 من عملاء بنك نيجيريا، كما اعتمد الباحث في التحليل على استخدام نمذجة المعادلة الهيكلية SEM بالبرنامج الإحصائي للعلوم الاجتماعية SPSS وبرنامج PLS-SMART.

توصلت الدراسة إلى عدة نتائج جاء أهمها أن كل من متغيري الأمن والخصوصية كان لهما تأثير إيجابي كبير على ثقة العملاء، حيث أن بعد الخصوصية تمتع بأعلى مستوى من التأثير والأهمية على جودة الخدمات الإلكترونية المصرفية، كما تم التأكيد على أن عامل ثقة العملاء له أهمية بالغة في الخدمات الإلكترونية المصرفية، ولا يمكن الاستغناء عنه في النموذج، بالإضافة إلى أن طلاب مؤسسات التعليم العالي هم يمثلون أكبر شريحة في البنك محل الدراسة يجب التركيز على أفضل طريقة لإرضائهم.

03-دراسة: Qais Amiri et al، (2021)، بعنوان:

Explore the Relationship between Security Mechanisms and Trust in E-Banking: A Systematic Review".

"اكتشاف العلاقة بين آليات الأمن والثقة في الخدمات الإلكترونية المصرفية: مراجعة منهجية".[2]

هدفت الدراسة إلى تطوير إطار نظري من أجل فحص العلاقة بين الأمن والثقة في الإنترنت في سياق الخدمات الإلكترونية المصرفية بالأردن، ولتحقيق أهداف الدراسة أستخدم المنهج الوصفي التحليلي من خلال التركيز على الإطار النظري بالاعتماد على الدراسات السابقة التي ترتكز على آليات القضايا الأمنية للخدمات الإلكترونية المصرفية، والتي درست الأبعاد الأمنية التالية: السرية، والتوافر والديمومة، وعدم الإنكار (الأثر)، الخصوصية،

[1] Ibrahim Maimunatu, Umar Muazu, **"Security and Privacy Dimension as Predictor of Internet Banking E-Service Quality on Customer Trust"**, International Journal of Innovative Science and Research Technology, ISSN N 2456-2165, Vol 6, N 11, 2021, PP 879-891, Https://www.ijisrt.com, Retrieved: 16-03-2022, 23:15.

[2] Qais Hamouri, Tahaer Majali, Damaithan Almajali, Abdalrazzaq Aloqool, Jassim Ahmad Al-Gasawneh, **"Explore the Relationship between Security Mechanisms and Trust in E-Banking: A Systematic Review"**, Annals of R.S.C.B, ISSN: 1583-6258, Vol 25, N 6, 2021, PP 17083-17093, Https://annalsofrscb.ro, Retrieved: 17-03-2022, 23:15.

التصديق الرقمي (الإلكتروني)، ومعرفة تأثيرها على ثقة العملاء تجاه استخدام الأنظمة للخدمات الإلكترونية المصرفية بدولة الأردن.

توصلت الدراسة إلى عدة نتائج جاء أهمها أن الثقة عامل مهم يؤثر على تبني العملاء لأي تقنية، مع خروج الدراسة بنموذج نظري متكامل ومتمم للدراسات السابقة في هذا المجال.

04-دراسة: Hamed Amiri، Deepti Dabas Hazarika، (2020)، بعنوان:

"Investigating The Effect Of Trust In Accepting Electronic Services: A Case of New Kabul Bank".

"التحقيق في تأثير الثقة على قبول الخدمات الإلكترونية: حالة بنك كابول الجديد".[1]

هدفت الدراسة إلى فحص دور الثقة في قبول الخدمات الإلكترونية ونية الاستخدام في قطاع الخدمات البنكية، ولتحقيق أهداف الدراسة أستخدم المنهج الوصفي التحليلي، وكانت أداة الدراسة عبارة عن الاستبانة وزعت على عينة اختيرت عشوائيا بلغت 450 من عملاء بنك كابول الجديد بدولة أفغانستان، كما اعتمد الباحث في التحليل على استخدام البرنامج الإحصائي للعلوم الاجتماعية SPSS V18.

توصلت الدراسة إلى عدة نتائج جاء أهمها أن هناك أربعة عوامل رئيسية تؤثر في نية الاستخدام تتمثل في الميل إلى الثقة، الثقة في تكنولوجيا المعلومات، الثقة في الحكومة، المخاطر المتصورة، حيث أن متغير الثقة في تكنولوجيا المعلومات له أكبر تأثير على نية الاستخدام، وأن شعور العملاء بالمخاطرة يؤدي إلى انخفاض نية الاستخدام ومن الأسباب الرئيسية لذلك عدم إلمام كثير من العملاء بالمعلومات التقنية.

05-دراسة: Mahdi Nasr Esfahani، (2019)، بعنوان:

"E-Bank Services: Analyzing the Effect of E-Bank Service on E-Trust with E-Security Approach."

"الخدمات الإلكترونية المصرفية: تحليل تأثير خدمة المصرف الإلكتروني على الثقة الإلكترونية من خلال نهج الأمن الإلكتروني".[2]

هدفت الدراسة إلى معرفة مدى تأثير أبعاد الخدمة الإلكترونية المصرفية على الثقة الإلكترونية للعملاء من خلال نهج الأمن الالكتروني، ولتحقيق أهداف الدراسة أستخدم المنهج الوصفي التحليلي، وكانت أداة الدراسة

---

[1] Amiri, Hazarika," Deepti Dabas Hazarik, **Investigating The Effect Of Trust In Accepting Electronic Services : A Case Of New Kabul Bank "**, European Journal of Molecular & Clinical Medicine, University of Granada, Spain, Vol 7, N 6, 2020, PP 1947-1958.

[2] Mahdi Nasr Esfahani, **"E-Bank Services : Analyzing the Effect of E-Bank Service on E-Trust with E-Security Approach "**,European Research Studies Journal, Department of the University of Malta, Vol 202, N 01, 2019, PP 158-166.

عبارة عن الاستبانة وزعت على عينة اختيرت عشوائيا بلغت 260 من عملاء بنك ميلي بإيران، كما اعتمد الباحث في التحليل على استخدام البرنامج الإحصائي للعلوم الاجتماعي SPSS V16.

توصلت الدراسة إلى عدة نتائج جاء أهمها أن كل بعد من أبعاد الخدمة الإلكترونية المصرفية يؤثر على الثقة، وأن العملاء راضون بشكل عام عن جودة الخدمات الإلكترونية المصرفية لبنك ميلي بإيران، وأن المزايا العديدة للخدمة الإلكترونية المصرفية على رأسها أحدث التقنيات والسلامة والأمن الذي يعتمد على نموذج يساعد على الكشف المبكر الذي لإهمال العملاء أو استهدافهم من خلال الذكاء الاصطناعي أو التعلم القائم على الآلة وبهذا يتم منع الخرق الأمني على الخدمات الإلكترونية المصرفية وهذا ما أدى إلى خفض النفقات وتوسع الأنشطة التسويقية وزيادة ثقة العملاء.

06-دراسة: Musbah Abdulkarim et al (2019)، بعنوان:

"Acceptance of Website Security on E-banking".

"قبول أمن الموقع الإلكتروني على الخدمات الإلكترونية المصرفية ".[1]

هدفت الدراسة إلى التعرف وفهم التأثير الحقيقي للأمن على مستخدمي الخدمات الإلكترونية المصرفية، إضافة الى تبيان علاقته بسلوك المستخدم تجاه قبول الخدمات الإلكترونية المصرفية، حيث يستعرض هذا البحث دراسات معمقة سابقة حول العوامل الأمنية المؤثرة في الخدمات الإلكترونية المصرفية (الثقة الأمنية، المخاطر، استراتيجية الحماية)، كما اتبعت الباحثة المنهج الوصفي التحليلي.

توصلت الدراسة إلى مجموعة من النتائج أبرزها: أن ثقة المستخدم ومخاوف الخصوصية لها أعلى نسبة تأثير على سلوك المستخدم تجاه قبول أي خدمة إلكترونية مصرفية، كما أن المشكلات الأمنية يمكن أن تؤدي إلى تقليل ثقة العملاء وبذلك يقل عدد مستخدمي الخدمات الإلكترونية المصرفية.

07-دراسة Azizi Muamer، (2018)، بعنوان:

"Pengaruh Persepsi Manfaat, Persepsi Kemudahan Penggunaan Dan Kemudahan, Kepercayaan Dan Persepsi Risiko Terhadap Minat Masyarakat Menggunakan Fasilitas Electronic Banking Bank Syariah Dengan Kepercayaan Sebagai Variabel Intervening, Studi Kasus Masyarakat Kamaran Ungaran Timur Kabupaten Semarang".

[1] Musbah abdulkarim, Musbah Ataya, Musab Ali, **"Acceptance of Website Security on E-banking"**, IEEE 10th Control and system Graduate Research Colloquium (ICSGRC), Shah Alam, Malaysia, 2-3 August 2019, P 228-233. https://ieeemy.org/section/2019-10th-ieee-control-and-system-graduate-research-colloquium-icsgrc-2019, Retrieved: 01-02-2022, 20:10.

"تأثير تصورات الفائدة، سهولة الاستخدام، المخاطر على قرارات العملاء في استخدام الخدمات المصرفية الإلكترونية من خلال الثقة كمتغير وسيط، دراسة حالة عملاء بنك الشارقة مقاطعة سيمار بأونجار أندونيسيا".[1]

هدفت الدراسة إلى اختبار ما إذا كان هناك تأثير ملحوظ على تصورات الفائدة، سهولة الاستخدام، المخاطر على قرار استخدام العملاء لمنتجات الخدمات الإلكترونية المصرفية مع الثقة كمتغير وسيط لبنك الشارقة PT BNI مقاطعة سيمار بأونجار بإندونيسيا، فكانت الدراسة الميدانية من خلال جمع عينات مستهدفة على أساس القدرة والكفاءة والفهم الحقيقي في المجال، بلغ عددها 155 عميل من خلال توزيع الاستبانة عليهم، كما اتبع الباحث المنهج الوصفي باستخدام البرنامج الإحصائي IBM SPSS 20 مع تحليل المسار.

توصلت الدراسة إلى مجموعة من النتائج أبرزها : أن كل من متغير الفائدة ومتغير سهولة الاستخدام ومتغير المخاطر لهم تأثير هام على اتخاذ قرار استخدام الخدمات الإلكترونية المصرفية من قبل العملاء وهذا بعد تعزيز متغير الثقة، كون هاته المعاملات تنطوي على مخاطر سيبرانية، كما توصلت الدراسة إلى أن هاته المتغيرات وهي مجتمعة معا تؤثر قطعا على قرار استخدام الخدمات الإلكترونية المصرفية ما يدل على أن مساهمة اختلاف المتغيرات المستقلة هي قادرة على تفسير تباين المتغير التابع من خلال نسبة 43،2%، بينما النسبة المتبقية 56،8% هي مفسرة بالمتغيرات الموجودة خارج نموذج البحث.

08-دراسة: Miska Laakkonen، (2017)، بعنوان:

"Elements of Trust and Their Impact on Purchase Intention and Customer Loyalty of Online Service Users-Cyber Security Perspective".

"عناصر الثقة وأثرها على نية الشراء للعميل وولاء مستخدمي الخدمة عبر الإنترنت – منظور الأمن السيبراني"[2]

هدفت الدراسة إلى تحليل العناصر المختلفة التي تساهم في الثقة والعناصر الأخرى التي تعتبر ذات صلة بالثقة التي يتصورها مستخدمي الخدمة عبر الإنترنت، ومعرفة تأثير هاته الثقة على نجاح الخدمة عبر الإنترنت،

[1] Azizi Muamer, **"Pengaruh Persepsi Manfaat, Persepsi Kemudahan Penggunaan Dan Kemudahan, Kepercayaan Dan Persepsi Risiko Terhadap Minat Masyarakat Menggunakan Fasilitas Electronic Banking Bank Syariah Dengan Kepercayaan Sebagai Variabel Intervening, Studi Kasus Masyarakat Kecamatan Ungaran Timur Kabupaten Semarang"**, International Islamic University Malaysia, College of Islamic Economics and Business, Islamic Banking Institute, Master's Thesis Electronic Banking Services, Malaysia,2018.

[2] **Miska Laakkonen**, **"Elements of Trust and Their Impact on Purchase Intention and Customer Loyalty of Online Service Users-Cyber Security Perspective",** Master's Thesis is to School of Science, Department of Computer Science, Aalto University, Finland, 2017, Https://aaltodoc.aalto.fi/bitstream/hadle/123456789/29197, Retrieved: 20-01-2022, 21:45.

والهدف الرئيسي من هذه الدراسة هو العثور على عناصر الثقة التي تؤثر على نية الشراء الأولية وولاء العملاء مستخدمي الخدمات عبر الإنترنت، والهدف الثانوي هو مقارنة تأثير عناصر الثقة المختلفة واكتشاف عناصر الثقة الأكثر أهمية لنجاح أي موقع إلكتروني عبر الإنترنت وكل هذا من منظور الأمن السيبراني، ولتحقيق أهداف الدراسة أستخدم المنهج الوصفي التحليلي، وكانت أداة الدراسة عبارة عن الاستبانة الإلكترونية وزعت على عينة من مستخدمي الخدمات عبر الإنترنت لسكان دولة فنلندا الذين تتراوح أعمارهم ما بين 15-69 عاما، حيث بلغت 779 مفردة بنسبة استرجاع 95%، كما اعتمد الباحث في التحليل على استخدام البرنامج الإحصائي للعلوم الاجتماعية SPSS.

توصلت الدراسة إلى عدة نتائج جاء أهمها أن الثقة عبر الإنترنت هي أحد أهم عوامل التأثير على نية الشراء وولاء العملاء لاستخدام الخدمة عبر الإنترنت، بينما هناك عوامل عديدة تساهم في الثقة التي يتصورها مستخدمو الخدمة عبر الإنترنت منها: الخصوصية، الأمان، السمعة، سهولة الاستخدام، وهي تسمى العناصر المركزية التي تؤثر على الثقة في استخدام الخدمة عبر الإنترنت ويجب أن يأخذها كل مقدم خدمة في الاعتبار عند تطوير خدمة جديدة على موقع الإنترنت، كما أنه يوجد عدة طرق لزيادة الثقة وهذا من خلال تنمية العناصر السالفة الذكر، ومن جهة أخرى تقليل تأثيرها السلبي المحتمل على الثقة المتصورة عبر الإنترنت، كما كان للخصوصية والأمان دور رئيسي في التأثير على الثقة في الخدمة عبر الإنترنت، وأي ضرر يلحق بهما مثل انتهاك البيانات الشخصية للمستخدمين، فهذا يمس بالسمعة وينعكس هذا على قابلية استخدام الخدمة.

09-دراسة: Mohammed Al-Sharafi et al، (2016)، بعنوان:

"The Effect of Security and Privacy Perception on Customers Trust to Accept Internet Banking Services: An Extension of TAM".

"تأثير تصور الأمن والخصوصية على ثقة العملاء في قبول الخدمات المصرفية عبر الإنترنت: نموذج تقبل التكنولوجيا TAM".[1]

هدفت الدراسة إلى دراسة كل من عامل الأمن والخصوصية وتأثيرها على ثقة العملاء الأردنيين لقبول الخدمات المصرفية عبر الإنترنت، ولتحقيق أهداف الدراسة أستخدم المنهج الوصفي التحليلي، وكانت أداة الدراسة عبارة عن الاستبانة وزعت على عينة اختيرت عشوائيا بلغت 198 من عملاء بنك ميلي بإيران، كما اعتمد الباحث في

[1] Mohammed Al-Sharafi, Ruzaini Arsha, Emad Abu-Shanab, Nabil Elayah, **"The Effect of Security and Privacy Perception on Customers Trust to Accept Internet Banking Services: An Extension of TAM"**, Journal of Engineering and Applied Sciences, Britain, Vol 11, N 3, 2016, PP 545-552.

التحليل على استخدام نمذجة المعادلة الهيكلية SEM بالبرنامج الإحصائي للعلوم الاجتماعية V21 AMOS.

توصلت الدراسة إلى عدة نتائج جاء أهمها أن الثقة لها تأثير إيجابي على النية السلوكية لاستخدام الخدمات المصرفية عبر الإنترنت، حيث أثر كل من عنصر فائدة الاستخدام والأمن والخصوصية بشكل كبير على ثقة العملاء المتصورة، أما بعد سهولة الاستخدام المتصورة فشل في توقع نية الأردنيين لاستخدام الخدمات المصرفية عبر الإنترنت.

10-دراسة: Gbadebo Maruf Salimon et al، (2015)، بعنوان:

"The Impact of Perceived Security on E-Trust, E-Satisfaction and Adoption of Electronic Banking in Nigeria: A Conceptual Review".

"تأثير الأمن المتصور على الثقة الإلكترونية والرضا الالكتروني في اعتماد الخدمات الإلكترونية المصرفية في نيجيريا".[1]

هدفت الدراسة إلى تحديد ومناقشة بعض العوامل المهمة من أجل تبني الخدمات الإلكترونية المصرفية خاصة بعد تطور مجال تكنولوجيا المعلومات وسلوك المستهلك ومن بين هاته العوامل المتصورة: الأمن السيبراني، الرضا والثقة الالكترونيين، ففي هذه الدراسة تم الاعتماد على المنهج الوصفي من خلال الكشف عن إطار مفاهيمي متعلق بالمتغيرات ومراجعة بعض الأدبيات ووصف طبيعة العلاقة وتحليل كل من عامل الأمن السيبراني، الرضا، الثقة في تبني الخدمات الإلكترونية المصرفية والخروج باستنتاجات وتوصيات.

أظهرت النتائج أن الثقة والرضا الإلكترونيين يعززان العلاقة بين الأمن المتصور وبين تبني الخدمات الإلكترونية المصرفية في نيجيريا، نظرا لكون طبيعة تقديم الخدمات المصرفية عبر الإنترنت تؤدي إلى انعدام الثقة وعدم اليقين لبعض العملاء، لذا فالثقة والرضا شرطين أساسين في بيئة الإنترنت أو أي نشاط تجاري آخر حيث يتم تبادل المعلومات الحساسة.

[1] Maruf Gbadebo Salimon, Rushami Zien Yusoff, Sany Sanuri Mohd Mokhtar,**" The Impact of Perceived Security on E-Trust, E-Satisfaction and Adoption of Electronic Banking in Nigeria: A Conceptual Review",** IOSR Journal of Business and Management (IOSR-JBM), University Utara Malaysia, Vol 1, N 1, 2015, PP 64-69.

مقارنة الدراسة الحالية مع الدراسات السابقة والقيمة المضافة للبحث

بغرض الكشف عن أهم أوجه التشابه والاختلاف بين الدراسة الحالية والدراسات السابقة ذات الصلة بالموضوع، قام الطالب بإعداد جداول لتوضيح هذه المقارنة، بدءا بالدراسات السابقة باللغة العربية، ثم الدراسات السابقة باللغة الأجنبية، وكذا تبيان القيمة المضافة للبحث الحالي.

جدول رقم (I): أهم أوجه التشابه والاختلاف بين الدراسة الحالية والدراسات السابقة.

الدراسة	أوجه التشابه	أوجه الاختلاف
عمرو أحمد نور الدين (2022)	– الدراسة في تخصص العلوم الاقتصادية "التسويق". – تناولت الدراسة المتغير التابع: "الخدمات الإلكترونية المصرفية". –تناولت الدراسة المتغير الوسيط: "الثقة". – استخدم الباحث المنهج الوصفي التحليلي. – تم جمع البيانات بواسطة الاستبيان. –تم تحليل البيانات بواسطة نمذجة المعادلات الهيكلية (SEM). –عينة الدراسة: عملاء المصرف. – الدراسة تمت في بنك عمومي.	– هدفت الدراسة إلى التعرف على الدور الوسيط لتوقعات الثقة في العلاقة بين المخاطر المدركة واستخدام الخدمات الإلكترونية المصرفية. – المتغير المستقل: "المخاطر المدركة". – العينة مكونة من: 384 مفردة. – استخدم الباحث البرنامج الإحصائي (AMOS). – أجريت الدراسة بدولة مصر العربية. – الفترة الزمنية: (2022). – أبرز نتائج الدراسة تحدثت عن: وجود تأثير معنوي إيجابي لتوقعات الثقة على استخدام الخدمات الإلكترونية المصرفية، فعندما ترتفع توقعات الثقة يرتفع استخدام الخدمات الإلكترونية المصرفية، كما أن التأثير هو تأثير معنوي سلبي للمخاطر المدركة من العميل على استخدام الخدمات الإلكترونية المصرفية، أي عند ارتفاع المخاطر المدركة ينخفض استخدام الخدمات الإلكترونية المصرفية.
يبدري ربيعة (2022)	– تناولت الدراسة المتغير المستقل: "الأمن السيبراني".	– الدراسة في تخصص العلوم القانونية. – هدفت الدراسة إلى التعرف على مدى فعالية دور الأمن السيبراني في حماية المعاملات

يبدري ربيعة (2022)	– استخدمت الباحثة المنهج الوصفي التحليلي بدراسة النصوص القانونية. – الدراسة مست المنظمة المصرفية. – أجريت الدراسة بالجزائر.	المالية الإلكترونية المصرفية المبرمة في الشكل الإلكتروني. – المتغير التابع: "المعاملات المالية المصرفية". – لا تحتوي الدراسة متغير وسيط. – الفترة الزمنية: (2022). – أبرز نتائج الدراسة تحدثت عن: أن مجال الأمن السيبراني لا ينحصر داخل الحدود الجغرافية للدول، بل هو يشمل كافة الدول بغض النظر عن الحدود الترابية التي تفصل كل دولة عن نظيرتها، بالإضافة إلى التأكيد على أن الأمن السيبراني وسيلة أثبتت فعاليتها في حماية الأنظمة الرقمية من الهجمات الفيروسية الإلكترونية لقواعد البيانات الحساسة.
منير عبد الله مفلح البيشي (2021)	– تناولت الدراسة المتغير المستقل: "الأمن السيبراني". –تناولت الدراسة متغير: "الثقة". – استخدم الباحث المنهج الوصفي التحليلي. – تم جمع البيانات بواسطة الاستبيان.	– الدراسة في تخصص العلوم التربوية والنفسية. – هدفت الدراسة إلى معرفة واقع الأمن السيبراني في الجامعات السعودية وأثره في تعزيز الثقة الرقمية من وجهة نظر أعضاء هيئة التدريس. – تناولت الدراسة لبعد "الثقة" كمتغير تابع. – لا تحتوي الدراسة على متغير وسيط. – عينة الدراسة: أعضاء هيئة التدريس. – الدراسة تمت في الجامعة. – العينة مكونة من: 182 مفردة. – استخدم الباحث البرنامج الإحصائي (SPSS) فقط. – أجريت الدراسة بدولة السعودية العربية. – الفترة الزمنية: (2021).

منير عبد الله مفلح البيشي (2021)		– أبرز نتائج الدراسة تحدثت عن: أن واقع الأمن السيبراني بالجامعات السعودية من وجهة نظر أعضاء هيئة التدريس مرتفعا بنسبة (73،18%)، كما تبين أن مستوى الثقة الرقمية للجامعات السعودية من وجهة نظر أعضاء هيئة التدريس مرتفعا بنسبة (74،58%)، وتبين أن الأمن السيبراني في الجامعات السعودية يؤثر في تعزيز الثقة الرقمية حيث بلغت نسبة التأثير (46،70%).
بن صالح ماجدة (2021)	– الدراسة في تخصص العلوم الاقتصادية: تسويق الخدمات". – تناولت الدراسة المتغير التابع: "الخدمات الإلكترونية المصرفية". –تناولت الدراسة متغير: "ثقة العملاء". – استخدمت الباحثة المنهج الوصفي التحليلي. –تم تحليل البيانات بواسطة نمذجة المعادلات الهيكلية (SEM). –عينة الدراسة: عملاء مصرف. – الدراسة تمت في المجال المصرفي. – أجريت الدراسة بدولة الجزائر.	– هدفت الدراسة إلى التعرف على مجموعة العوامل المؤثرة على ثقة العملاء في الخدمات الإلكترونية المصرفية في الجزائر، مفترضة أن كل من: خصائص الخدمة، الأمان، السرية، سهولة الاستخدام، وخصائص البنك المتمثلة في سمعته وحجمه، وخصائص المستهلك المتمثلة في التجارب السابقة والكفاءة في استخدام الحاسب الآلي هي متغيرات مستقلة تؤثر على الثقة في الخدمات الإلكترونية المصرفية كمتغير تابع. – المتغير المستقل: "العوامل المؤثرة على الثقة". – تمت الدراسة على مجموعة من عملاء عدة بنوك. – تم جمع البيانات بواسطة الاستبيان والمقابلة. – عينة الدراسة مكونة من: 154 مفردة. – استخدمت الباحثة البرنامج الإحصائي (AMOS). – الفترة الزمنية: (2021).

بن صالح ماجدة (2021)		– بالنسبة لأبعاد المتغير المستقل، فالأمن هو عنصر واحد فقط من العوامل المؤثرة على ثقة العملاء المصرفيين. – أبرز نتائج الدراسة تحدثت عن: ثبوت كافة العوامل المقترحة، أن من أهم مقومات بناء الثقة في الخدمات الإلكترونية المصرفية هي الأمان والسرية التي لا زالت تشكل معضلة كبرى حتى على الدول العظمى التي تحتل المراتب الأولى في المجال البنكي رغم تشديد الإجراءات الأمنية والرقابية على مختلف المخاطر البنكية الناجمة عن التعاملات الإلكترونية، أما سهولة الاستخدام المدركة والتجارب السابقة للعميل المصرفي وكفاءته في استخدام الحاسب الآلي فهي عوامل يمكن التحكم فيها بتسهيل الإجراءات وتعريب المواقع وتبسيط المراحل اللازمة لتنفيذ العمليات الإلكترونية المصرفية، وبالنسبة لحجم وسمعة البنك المدركة فهما عاملان مهمان جدا لبناء الثقة في البنك أولا ثم الخدمات المقدمة إلكترونيا.
مروة فتحي السيد البغدادي (2021)	– الدراسة في تخصص العلوم الاقتصادية " إدارة الأعمال". – تناولت الدراسة المتغير المستقل: "الأمن السيبراني". – الدراسة تمت في المجال المصرفي.	– هدفت الدراسة إلى التعرف على أهم التحديات التي تواجه القطاع المالي وبشكل خاص المصرفي في دولة مصر، من أجل تحقيق الأمن السيبراني، والذي يلعب دورا محوريا في معالجة التحديات المستقبلية نظرا لاستخدامه كتكنولوجيا لإدارة الشبكات، الأمر الذي يساعد في تحقيق عدد من أهداف التنمية المستدامة: كتحسين إدارة استخدام المعدات وصيانتها، زيادة الإنتاج، توسيع نطاق الوصول

مروة فتحي السيد البغدادي (2021)		إلى المعلومات المتعلقة بالتفاعل الاقتصادي بين المؤسسات الخاصة والعامة. – لا تحتوي الدراسة على متغير وسيط. – استخدمت الباحثة المنهج الوصفي والمنهج المقارن. –عينة الدراسة: تمثلت في مجموعة من البنوك. – الفترة الزمنية: (2021). – أجريت الدراسة بدولة مصر العربية. – أبرز نتائج الدراسة تحدثت عن: أن الطبيعة المتطورة للمخاطر السيبرانية ليست قابلة للتنظيم بشكل محدد، كما أن القضايا الخاصة بالإنترنت (Cyber Issues) يمكن معالجتها من خلال اللوائح المتعلقة بالمخاطر التشغيلية ومختلف التقنيات، إضافة إلى أن التطور الحادث في المخاطر السيبرانية يحفز المؤسسات المالية على البحث المستمر والمكثف نحو اتخاذ إجراءات وقائية، الأمر الذي يؤدي إلى خلق حافز أكبر على الاستثمار بشكل مستمر في الأمن السيبراني.
حسن نجيب الرواش وآخرون (2020)	– الدراسة في تخصص العلوم الاقتصادية "التسويق". – تناولت الدراسة المتغير التابع: "الخدمات الإلكترونية المصرفية". – الدراسة تمت في المجال المصرفي. – استخدم الباحثون المنهج الوصفي التحليلي. – تم جمع البيانات بواسطة الاستبيان.	– هدفت الدراسة إلى التعرف إلى الأسباب التي تحد من استخدام الخدمات المصرفية عبر الإنترنت في الأردن، ومعرفة الخصائص الديموغرافية في مجال استخدامها، وهذا من خلال تحليل خمسة متغيرات هي: (الأمن والخصوصية، الثقة، سهولة الاستخدام، الفائدة المتوقعة، الاحتياجات البنكية). – المتغير المستقل في الدراسة: "محددات الاستخدام". – لا تحتوي الدراسة على متغير وسيط.

حسن نجيب الرواش وآخرون (2020)		– عينة الدراسة مكونة من: 302 مفردة لعملاء البنوك العاملين في الجامعات الخاصة (موظفين بالجامعات). – استخدم الباحث البرنامج الإحصائي (SPSS). – الفترة الزمنية: (2020). – أجريت الدراسة: بإقليم شمال دولة الأردن. – أبرز نتائج الدراسة تحدثت عن: عدم وجود فروقات ذات دلالة إحصائية على جميع مجالات الدراسة تبعا لمتغير الجنس، ووجود فروقات ذات دلال إحصائية لمجال الاحتياجات البنكية والمرحلة العمرية لخمسين سنة فأكثر، ووجود دلال إحصائية لمجال الفائدة المتوقعة والتحصيل العلمي دراسات عاليا.
الزهرة برة وجميلة حميدة (2019)	– تناولت الدراسة المتغير الوسيط: "الثقة". – استخدمت الباحثتين المنهج الوصفي التحليلي. – أجريت الدراسة بدولة الجزائر.	– الدراسة في تخصص العلوم القانونية والسياسية. – الدراسة تمت في مجال المعاملات الإلكترونية في كافة المجلات ولم تقتصر على الخدمات المصرفية. – هدفت الدراسة إلى التعرف على شهادة التصديق الالكتروني وتوضيح دورها في توثيق المعاملات الإلكترونية بصفة عامة والتجارة الإلكترونية بصفة خاصة لاسيما عبر شبكة الإنترنت من خلال تعزيز عنصر الثقة والأمان. – لا تحتوي الدراسة على متغير الأمن السيبراني ومتغير الخدمات للمصرفية الإلكترونية.

الزهرة برة وجميلة حميدة (2019)		– الفترة الزمنية: (2019). – أبرز نتائج الدراسة هي: أن شهادة التصديق الالكتروني تتمتع بقيمة قانونية وحجية كاملة في الإثبات شأنها شأن المحررات الرسمية وتعد دليلا تقنيا يعول عليه في الإثبات إذا ما توفرت فيها مجموعة من الشروط التي نص عليها القانون، في مقدمتها صدورها من جهة مختصة معتمدة، احتوائها على مجموعة من البيانات واستجابتها لمقتضيات الثقة والأمان.
محمد الشرفي وآخرون (2018)	– الدراسة في تخصص العلوم الاقتصادية "التسويق". – تناولت الدراسة المتغير التابع: "الخدمات الإلكترونية المصرفية". –تناولت الدراسة متغير: "ثقة العملاء". – الدراسة تمت في المجال المصرفي. – استخدم الباحثون المنهج الوصفي التحليلي. – تم جمع البيانات بواسطة الاستبيان. – العينة محل الدراسة: تمثلت في عملاء البنوك. –تم تحليل البيانات بواسطة نمذجة المعادلات الهيكلية (SEM).	– هدفت الدراسة إلى التحقيق في تأثير تصورات الأمن والخصوصية للعملاء على قبولهم اعتماد الخدمات الإلكترونية المصرفية بدولة الأردن، حيث ركزت الدراسة في العوامل التي تؤثر علا ثقة العملاء في قبول استخدام الخدمات المصرفية عبر الإنترنت، وقد اعتمد الباحثون على نموذج دراسة يدعم النموذج النظري TAM مطور يعكس بدقة العوامل التي تؤثر على ثقة العملاء في قبول واستخدام الخدمات الإلكترونية المصرفية. – المتغير المستقل في الدراسة: "ثقة العملاء وتصورهم لأمن خصوصيتهم". – لا تحتوي الدراسة على متغير وسيط. – عينة الدراسة مكونة من: 198 مفردة لعملاء البنوك. – استخدم الباحثون البرنامج الإحصائي (AMOS). – الفترة الزمنية: (2018). – أجريت الدراسة: بدولة الأردن.

محمد الشرفي وآخرون (2018)		– أبرز نتائج الدراسة تحدثت عن: أن للثقة أثر إيجابي على نية العملاء السلوكية لاعتماد الخدمات المصرفية عبر الإنترنت، علاوة على ذلك تصور العملاء لفائدتهم وأمن خصوصيتهم كان له أيضا تأثير كبير على ثقتهم، ومع ذلك فإن سهولة الاستخدام المتصورة للمستخدمين فشلت في ذلك.
عبد الله سيد ماهر بدوي (2013)	– الدراسة في تخصص العلوم الاقتصادية "إدارة الأعمال". –تناولت الدراسة متغير: "ثقة العملاء". – استخدم الباحث المنهج الوصفي التحليلي. – تم جمع البيانات بواسطة أداة الاستبيان. – تم تحليل البيانات بواسطة نمذجة المعادلات الهيكلية (SEM). – عينة الدراسة: عملاء المصرف. – الدراسة تمت في المجال المصرفي.	– هدفت الدراسة إلى قياس ثقة عملاء البنك على قبولهم التعامل المصرفي عبر الإنترنت، حيث اعتمد البحث على سؤالين بحثيين يتعلقان بالثقة كمفهوم متعدد الأبعاد يشمل ثلاثة أبعاد رئيسية (الأمانة، القدرة، النفع) تعمل كمؤشرات antécédents للثقة العامة (في البنك كمؤسسة، في الخدمة كمنتج، في الإنترنت كوسيط)، هذه الثقة تعتبر مؤشرا مباشرا لكل من الاتجاه نحو الاستخدام والنية السلوكية لاستخدام التعامل المصرفي عبر الإنترنت. – بعد "ثقة العملاء" متغير مستقل. – العينة مكونة من: 290 مفردة. – استخدم الباحث برنامج (AMOS). – أجريت الدراسة بالقاهرة دولة مصر العربية. – الفترة الزمنية: (2013). – أبرز نتائج الدراسة تحدثت عن: أن الثقة مفهوم متعدد الأبعاد (الأمانة، القدرة، النفع) تعمل كمؤشرات للثقة العامة في التعامل المصرفي عبر الإنترنت (البنك، الخدمة، الإنترنت) وتفسر 43% منها، كما تعتبر أحد أهم مؤشرات قبول التعامل المصرفي عبر

عبد الله سيد ماهر بدوي (2013)		الإنترنت، ولها تأثير معنوي مباشر على النية السلوكية لاستخدام التعامل المصرفي عبر الإنترنت. وأن النفع المدرك للبنك على الإنترنت هو أهم عوامل الثقة في التعامل المصرفي عبر الإنترنت، يليه الأمانة المدركة ثم القدرة المدركة للبنك عبر الإنترنت.
محمد عصمان، شريف مهدي (2011)	– الدراسة في تخصص العلوم الاقتصادية "إدارة الأعمال". – تناولت الدراسة المتغير المستقل: "الأمن السيبراني". – تناولت الدراسة المتغير التابع: "الخدمات الإلكترونية المصرفية". –تناولت الدراسة متغير: "ثقة العملاء". – استخدم الباحث المنهج الوصفي التحليلي. – تم جمع البيانات بواسطة الاستبيان. –عينة الدراسة: عملاء المصرف. – الدراسة تمت في المجال المصرفي.	– هدفت الدراسة إلى فحص ثقة وأمن الخدمات الإلكترونية المصرفية في البنوك التجارية السعودية، مع اجراء مقارنة لآراء العملاء السعوديين وغير السعوديين. – بعد " ثقة العملاء" متغير مستقل. – لا تحتوي الدراسة متغير وسيط. – العينة مكونة من: 418 مفردة. – عينة الدراسة: عملاء مجموعة من البنوك. – استخدم الباحث برنامج (SPSS) فقط. – أجريت الدراسة في أربعة مدن في المنطقة الشرقية للمملكة العربية السعودية. – الفترة الزمنية: (2011). – أبرز نتائج الدراسة تحدثت عن: وجود فروق ثقة كبيرة بين السعوديين وغير السعوديين في استخدام الخدمات الإلكترونية المصرفية، بما في ذلك أجهزة الصراف الآلي وبطاقات الائتمان والرسائل المصرفية النصية القصيرة عبر الهاتف والخدمات المصرفية الأخرى عبر الإنترنت، كما كشفت النتائج عن مدى ثقة عملاء البنوك السعودية بدرجة كبيرة باستخدام الخدمات الإلكترونية المصرفية مع اعتقادهم بقوة أنها أكثر أمانا مقارنة بنظيراتها من غير السعوديين، كما قدمت الدراسة أدلة تجريبية

محمد عصمان، شريف مهدي (2011)		جديدة تعزز فهمنا للثقة والأمان لتكنولوجيا الخدمات الإلكترونية المصرفية في البنوك الإلكترونية السعودية.
Khalid ،Khalil (2021)	– الدراسة في تخصص العلوم الاقتصادية "فلسفة إدارة الأعمال". – تناولت الدراسة المتغير المستقل: "الأمن السيبراني". – تناولت الدراسة المتغير التابع: "الخدمات الإلكترونية المصرفية". – استخدم الباحث المنهج الوصفي التحليلي. – تم جمع البيانات بواسطة الاستبيان. – الدراسة تمت في المجال المصرفي. – تم تحليل البيانات بواسطة نمذجة المعادلات الهيكلية (SEM).	– هدفت الدراسة إلى قياس العلاقة السببية لتكاليف الأمن السيبراني من خلال المتغيرات التالية: المنع/الكشف، الاستجابة، التطوير، الصيانة، على الأداء المالي للخدمات الإلكترونية المصرفية، وكذا فحص تأثير أداء ابتكار المنتج على الأداء المالي للخدمات الإلكترونية المصرفية، وكذا إيجاد متغير وسيط في علاقة تأثير أداء ابتكار المنتجات على تكاليف الأمن السيبراني وأداء الخدمات الإلكترونية المصرفية. – تناولت الدراسة متغير وسيط تمثل في "أداء ابتكار المنتجات". – العينة مكونة من: 550 مفردة. – عينة الدراسة: كوادر موظفي ثمانية بنوك. – استخدم الباحث البرنامج الإحصائي (SPSS) وبرنامج (AMOS). – أجريت الدراسة في مدن خيبر وإسلام أباد والبنجاب بدولة باكستان. – الفترة الزمنية: (2021). – أبرز نتائج الدراسة تحدثت عن: أن تكاليف الأمن السيبراني لها تأثير إيجابي كبير على الأداء المالي لابتكار المنتجات والخدمات الإلكترونية المصرفية، كما أن لابتكار المنتج تأثير إيجابي كبيرة على الأداء المالي للخدمات الإلكترونية المصرفية، بالإضافة إلى أداء ابتكار المنتج توسط جزئيا العلاقة بين تكاليف الأمن

Khalid ،Khalil (2021)		السيبراني وأداء التمويل المصرفي الإلكتروني، ومن هنا كان لتكاليف تأمين تكنولوجيا المعلومات (تكاليف الكشف والمنع) تأثير كبير على إنتاج المنتجات المصرفية الإلكترونية.
Ibrahim Maimunatu Umar Muazu (2021)	– الدراسة في تخصص العلوم الاقتصادية "التسويق". – تناولت الدراسة المتغير المستقل: "الأمن السيبراني". – تناولت الدراسة المتغير التابع: "الخدمات الإلكترونية المصرفية". – استخدم الباحث المنهج الوصفي التحليلي. – تم جمع البيانات بواسطة الاستبيان. – الدراسة تمت في المجال المصرفي. – عينة الدراسة: تمثلت في عملاء بنك واحد. – تم تحليل البيانات بواسطة نمذجة المعادلات الهيكلية (SEM). – استخدم الباحثين البرنامج الإحصائي (SPSS) وبرنامج (SMART PLS).	– هدفت الدراسة إلى تأكيد أن بعد الأمن والخصوصية كمؤشر لجودة الخدمات الإلكترونية المصرفية عبر الإنترنت على ثقة العملاء، ولعبها دورا رئيسيا في تحسين جود الخدمات وتحسين العملية المتعلقة بالصناعة المصرفية، مع فحص جودة ثقة العملاء باستخدام النموذج E-S-QUAL. – تناولت الدراسة لبعد الأمن السيبراني إلى جانبه بعد الخصوصية كمؤشرات لجودة الخدمات المصرفية. – تناولت الدراسة متغير "الثقة" كمتغير تابع. – لم تتناول الدراسة متغير وسيط. – العينة مكونة من: 379 مفردة. – أجريت الدراسة في دولة نيجيريا. – الفترة الزمنية: (2021). – أبرز نتائج الدراسة تحدثت عن: أن كل من متغيري الأمن والخصوصية كان لهما تأثير إيجابي كبير على ثقة العملاء، حيث أن بعد الخصوصية تمتع بأعلى مستوى من التأثير والأهمية على جودة الخدمات الإلكترونية المصرفية، كما تم التأكيد على أن عامل ثقة العملاء له أهمية بالغة في الخدمات الإلكترونية المصرفية، ولا يمكن الاستغناء عنه في النموذج، بالإضافة إلى أن طلاب مؤسسات التعليم العالي

		هم يمثلون أكبر شريحة في البنك محل الدراسة يجب التركيز على أفضل طريقة لإرضائهم.
Qais et al Amiri (2021)	– الدراسة في تخصص العلوم الاقتصادية "التسويق". – تناولت الدراسة المتغير المستقل: "الأمن السيبراني". – اتفقت الدراستين في أبعاد الأمن السيبراني الأربعة التالية: السرية، التوافر والديمومة، عدم الإنكار أي (تتبع الأثر)، الخصوصية. – استخدم الباحثون المنهج الوصفي التحليلي للدراسات النظرية السابقة مع اقتراح نموذج نظري متكامل. – الدراسة تمت في المجال المصرفي.	– هدفت الدراسة إلى تطوير إطار نظري من أجل فحص العلاقة بين الأمن والثقة في الإنترنت في سياق الخدمات الإلكترونية المصرفية بالأردن. – اختلفت الدراستين بالنسبة لأحد أبعاد المكونة لمتغير الأمن السيبراني حيث اعتمدت هذه الدراسة على بعد التصديق الرقمي بينما دراستنا اعتمدت على بعد التكنولوجيا المستخدمة وهو أشمل وأعم منه. – تناولت الدراسة لبعد "الثقة" كمتغير تابع. – لم تتناول الدراسة متغير وسيط. – أجريت الدراسة في دولة الأردن. – الفترة الزمنية: (2021). – أبرز نتائج الدراسة تحدثت عن: أن الثقة عامل مهم يؤثر على تبني العملاء لأي تقنية، مع خروج الدراسة بنموذج نظري متكامل ومتمم للدراسات السابقة في هذا المجال.
Hamed Amiri, Deepti Dabas Hazarika (2020)	– الدراسة في تخصص العلوم الاقتصادية "البنوك". – تناولت الدراسة المتغير التابع: "الخدمات الإلكترونية المصرفية". – تناولت الدراسة متغير: "الثقة". – استخدم الباحث المنهج الوصفي التحليلي. – تم جمع البيانات بواسطة الاستبيان. – الدراسة تمت في المجال المصرفي.	– هدفت الدراسة إلى فحص دور الثقة في قبول الخدمات الإلكترونية ونية الاستخدام في قطاع الخدمات البنكية. – تناولت الدراسة لبعد "الثقة" كمتغير مستقل. – لم تتناول الدراسة متغير وسيط. – العينة مكونة من: 450 مفردة. – أجريت الدراسة في مدينة كابول بدولة أفغانستان. – الفترة الزمنية: (2020).

Hamed Amiri, Deepti Dabas Hazarika (2020)	- عينة الدراسة: تمثلت في عملاء بنك واحد.	- استخدم الباحثين البرنامج الإحصائي (SPSS) فقط. - أبرز نتائج الدراسة تحدثت عن: هناك أربعة عوامل رئيسية تؤثر في نية الاستخدام تتمثل في الميل إلى الثقة، الثقة في تكنولوجيا المعلومات، الثقة في الحكومة، المخاطر المتصورة، حيث أن متغير الثقة في تكنولوجيا المعلومات له أكبر تأثير على نية الاستخدام، وأن شعور العملاء بالمخاطرة يؤدي إلى انخفاض نية الاستخدام ومن الأسباب الرئيسية لذلك عدم إلمام كثير من العملاء بالمعلومات التقنية.
Mahdi Nasr Esfahani (2019)	- الدراسة في تخصص العلوم الاقتصادية "التسويق". - تناولت الدراسة جميع متغيرات الدراسة الثلاثة. - استخدم الباحث المنهج الوصفي التحليلي. - تم جمع البيانات بواسطة الاستبيان. - الدراسة تمت في المجال المصرفي. - عينة الدراسة: تمثلت في عملاء بنك واحد.	- هدفت الدراسة إلى معرفة مدى تأثير أبعاد الخدمة المصرفية الإلكترونية على الثقة الإلكترونية للعملاء من خلال نهج الأمن الالكتروني. - تناولت الدراسة متغير "الخدمة الإلكترونية المصرفية "كمتغير مستقل. - تناولت الدراسة لبعد "الثقة"كمتغير تابع. - تتناول الدراسة لبعد "الأمن السيبراني"كمتغير وسيط. - العينة مكونة من: 260 مفردة. - أجريت الدراسة في دولة إيران. - الفترة الزمنية: (2019). - استخدم الباحثين البرنامج الإحصائي (SPSS) فقط. - أبرز نتائج الدراسة تحدثت عن: أن كل بعد من أبعاد الخدمة الإلكترونية المصرفية يؤثر على الثقة، وأن العملاء راضون بشكل عام عن جودة الخدمات الإلكترونية المصرفية لبنك ميلي، وأن

Mahdi Nasr Esfahani (2019)		المزايا العديدة للخدمة المصرفية الإلكترونية على رأسها أحدث التقنيات والسلامة والأمن الذي يعتمد على نموذج يساعد على الكشف المبكر لإهمال العملاء أو استهدافهم من خلال الذكاء الاصطناعي أو التعلم القائم على الآلة وبهذا يتم منع الخرق الأمني على الخدمات الإلكترونية المصرفية وهذا ما أدى إلى خفض النفقات وتوسع الأنشطة التسويقية وزيادة ثقة العملاء.
Musbah Abdulkarim et al (2019) **Musbah Abdulkarim et al (2019)**	– الدراسة في تخصص العلوم الاقتصادية "فلسفة إدارة الأعمال". – تناولت الدراسة المتغير المستقل: "الأمن السيبراني". – تناولت الدراسة المتغير التابع: "الخدمات الإلكترونية المصرفية". – استخدم الباحث المنهج الوصفي التحليلي. – الدراسة تمت في المجال المصرفي. – عينة الدراسة: تمثلت في عملاء المصرف.	– هدفت الدراسة إلى التعرف وفهم التأثير الحقيقي للأمن على مستخدمي الخدمات الإلكترونية المصرفية، إضافة الى تبيان علاقته بسلوك المستخدم تجاه قبول الخدمات الإلكترونية المصرفية، حيث يستعرض هذا البحث دراسات معمقة سابقة حول العوامل الأمنية المؤثرة في الخدمات الإلكترونية المصرفية (الثقة الأمنية، المخاطر، استراتيجية الحماية). – لم تتناول الدراسة لمتغير وسيط. – أجريت الدراسة في دولة ماليزيا. – الفترة الزمنية: (2019). – أبرز نتائج الدراسة تحدثت عن: أن ثقة المستخدم ومخاوف الخصوصية لها أعلى نسبة تأثير على سلوك المستخدم تجاه قبول أي خدمة مصرفية إلكترونية، كما أن المشكلات الأمنية هي تؤدي إلى تقليل ثقة العملاء وبذلك يقل عدد مستخدمي الخدمات الإلكترونية المصرفية.

Azizi Muamer (2018)	– الدراسة في تخصص العلوم الاقتصادية "الخدمات المصرفية الإلكتروني". – تناولت الدراسة المتغير التابع: "الخدمات الإلكترونية المصرفية". – تناولت الدراسة المتغير الوسيط: "ثقة العملاء". – استخدم الباحث المنهج الوصفي التحليلي. – تم جمع البيانات بواسطة الاستبيان. – الدراسة تمت في المجال المصرفي. – عينة الدراسة: تمثلت في عملاء بنك واحد.	– هدفت الدراسة إلى اختبار ما إذا كان هناك تأثير ملحوظ على تصورات الفائدة، سهولة الاستخدام، المخاطر على قرار استخدام العملاء لمنتجات الخدمات الإلكترونية المصرفية مع الثقة كمتغير وسيط لبنك الشارقة PT BNI مقاطعة سيمار بأونجار بأندونيسيا. – تناولت الدراسة المتغيرات المستقلة التالية: "تصور الفائدة، سهولة الاستخدام، المخاطر". – العينة مكونة من: 155 مفردة. – أجريت الدراسة في مقاطعة سيمار بأونجار بأندونيسيا. – الفترة الزمنية: (2018). – استخدم الباحثين البرنامج الإحصائي (SPSS) فقط. – أبرز نتائج الدراسة تحدثت عن: أن كل من متغير الفائدة ومتغير سهولة الاستخدام ومتغير المخاطر لهم تأثير هام على اتخاذ قرار استخدام الخدمات الإلكترونية المصرفية من قبل العملاء وهذا بعد تعزيز متغير الثقة، كون هاته المعاملات تنطوي على مخاطر سيبرانية، كما توصلت أيضا إلى أن هذه المتغيرات وهي مجتمعة معا تؤثر على قرار استخدام الخدمات الإلكترونية المصرفية ما يدل على أن مساهمة اختلاف المتغيرات المستقلة هي قادرة على تفسير تباين المتغير التابع من خلال نسبة 43،2%، بينما المتبقية 56،8% هي مفسرة بالمتغيرات الموجودة خارج نموذج البحث.
Azizi Muamer (2018)		

Miska Laakkonen (2017)	– الدراسة في تخصص العلوم الاقتصادية "الخدمات المصرفية الإلكتروني". – تناولت الدراسة لمتغير الأمن السيبراني". – تناولت الدراسة للعوامل المؤثرة على "الثقة" من منظور بعد "الأمن السيبراني". – استخدم الباحث المنهج الوصفي التحليلي. – تم جمع البيانات بواسطة الاستبيان.	– هدفت الدراسة إلى تحليل العناصر المختلفة التي تساهم في الثقة والعناصر الأخرى التي تعتبر ذات صلة بالثقة التي يتصورها مستخدمي الخدمة عبر الإنترنت، ومعرفة تأثير هاته الثقة على نجاح الخدمة عبر الإنترنت، والهدف الرئيسي من هذه الدراسة هو العثور على عناصر الثقة التي تؤثر على نية الشراء الأولية وولاء العملاء مستخدمي الخدمات عبر الإنترنت، والهدف الثانوي هو مقارنة تأثير عناصر الثقة واكتشاف الأكثر عناصر أهمية لنجاح أي موقع إلكتروني عبر الإنترنت وكل هذا من منظور الأمن السيبراني. – الدراسة مست جميع مجالات نشاط الخدمة الإلكترونية بما فيها المصرفية " بمعنى الخدمات الإلكترونية بصفة عامة". – تناولت الدراسة لبعد "الثقة" كمتغير مستقل. – عينة الدراسة مكونة من: 779 مفردة. – عينة الدراسة: تمثلت في مستخدمي الخدمات عبر الانترنت الذين تتراوح أعمارهم ما بين (15-65 عاما). – أجريت الدراسة في دولة فنلندا. – الفترة الزمنية: (2017). – استخدم الباحث البرنامج الإحصائي (SPSS) فقط – أبرز نتائج الدراسة تحدثت عن: أن الثقة عبر الإنترنت هي أحد أهم عوامل التأثير على نية الشراء وولاء العملاء لاستخدامها، بينما هناك عوامل عديدة تساهم في الثقة التي يتصورها مستخدمو الخدمة عبر الإنترنت:

Miska Laakkonen (2017)		كالخصوصية، الأمان، السمعة، سهولة الاستخدام، وهي تسمى العناصر المركزية التي تؤثر على الثقة في استخدام الخدمة عبر الإنترنت ويجب أن يأخذها كل مقدم خدمة في الاعتبار عند تطوير خدمة جديدة على موقع الإنترنت، كما أنه يوجد عدة طرق لزيادة الثقة وهذا من خلال تنمية العناصر السالفة الذكر، ومن جهة أخرى تقليل تأثيرها السلبي المحتمل على الثقة المتصورة عبر الإنترنت، كما كان للخصوصية والأمان دور رئيسي في التأثير على الثقة في الخدمة عبر الإنترنت، وأي ضرر يلحق بهما مثل انتهاك بيانات للمستخدمين، فهذا يمس بالسمعة وينعكس على قابلية استخدام الخدمة.
Mohammed Al-Sharafi et al (2016)	– الدراسة في تخصص العلوم الاقتصادية "البنوك". – تناولت الدراسة المتغير المستقل: "الأمن السيبراني" – تناولت الدراسة المتغير التابع: "الخدمات الإلكترونية المصرفية". – تناولت الدراسة لبعد " الثقة" كمتغير وسيط. – استخدم الباحث المنهج الوصفي التحليلي. – تم جمع البيانات بواسطة الاستبيان. – الدراسة تمت في المجال المصرفي. – عينة الدراسة: تمثلت في عملاء بنك واحد.	– هدفت الدراسة إلى دراسة كل من عامل الأمن والخصوصية وتأثيرها على ثقة العملاء الأردنيين لقبول الخدمات المصرفية عبر الإنترنت. – تناولت الدراسة لبعد الأمن السيبراني إلى جانبه الخصوصية كمتغيرين مستقلين. – تم الاعتماد في الدراسة على نموذج تقبل التكنولوجيا (TAM). – العينة مكونة من: 198 مفردة. – أجريت الدراسة في دولة إيران. – الفترة الزمنية: (2016). – استخدم باحثين برنامج (AMOS). – أبرز نتائج الدراسة تحدثت عن: أن الثقة لها تأثير إيجابي على النية السلوكية لاستخدام الخدمات المصرفية عبر الإنترنت، حيث أثر كل

	- تم تحليل البيانات بواسطة نمذجة المعادلات الهيكلية (SEM).	من عنصر فائدة الاستخدام والأمن والخصوصية بشكل كبير على ثقة العملاء المتصورة، كما أن بعد سهولة الاستخدام المتصورة فشل في توقع نية الأردنيين لاستخدام الخدمات المصرفية عبر الإنترنت وبهذا فهو مؤشر غير مهم.
Gbadebo Maruf Salimon et al (2015)	- الدراسة في تخصص العلوم الاقتصادية "التسويق". - تناولت الدراسة المتغير المستقل: "الأمن السيبراني". - تناولت الدراسة المتغير التابع: "الخدمات الإلكترونية المصرفية". - الدراسة تمت في المجال المصرفي. - استخدم الباحث المنهج الوصفي التحليلي من خلال الكشف عن إطار مفاهيمي متعلق بالمتغيرات ومراجعة بعض الأدبيات ووصف طبيعة العلاقات فيما بينها مع تحليلها باقتراح نموذج نظري متكامل.	- هدفت الدراسة إلى تحديد ومناقشة بعض العوامل المهمة من أجل تبني الخدمات الإلكترونية المصرفية خاصة بعد تطور مجال تكنولوجيا المعلومات وسلوك المستهلك ومن بين هاته العوامل المتصورة: الأمن السيبراني، الرضا والثقة الالكترونيين. - تناولت الدراسة لبعدين وسيطيين معا وهما: "الثقة والرضا". - أجريت الدراسة في دولة نيجيريا. - الفترة الزمنية: (2015). - أبرز نتائج الدراسة تحدثت عن: أن الثقة والرضا الإلكترونيين يعززان العلاقة بين الأمن المتصور وبين الخدمات الإلكترونية المصرفية في نيجيريا، نظرا لكون طبيعة تقديم الخدمات الإلكترونية المصرفية تؤدي إلى انعدام الثقة وعدم اليقين لبعض العملاء، لذا فالثقة والرضا شرطين أساسين في بيئة الإنترنت، حيث يتم تبادل المعلومات الحساسة.

المصدر: من إعداد الطالب بالاعتماد على الدراسات السابقة.

ما يميز الدراسة الحالية عن الدراسات السابقة:

من خلال استعراض أوجه التشابه والاختلاف بين الدراسة الحالية والدراسات السابقة، موضوع بحثنا ينفرد بطابعه الخاص والمميز عن سابقيه من خلال العناصر التالية:

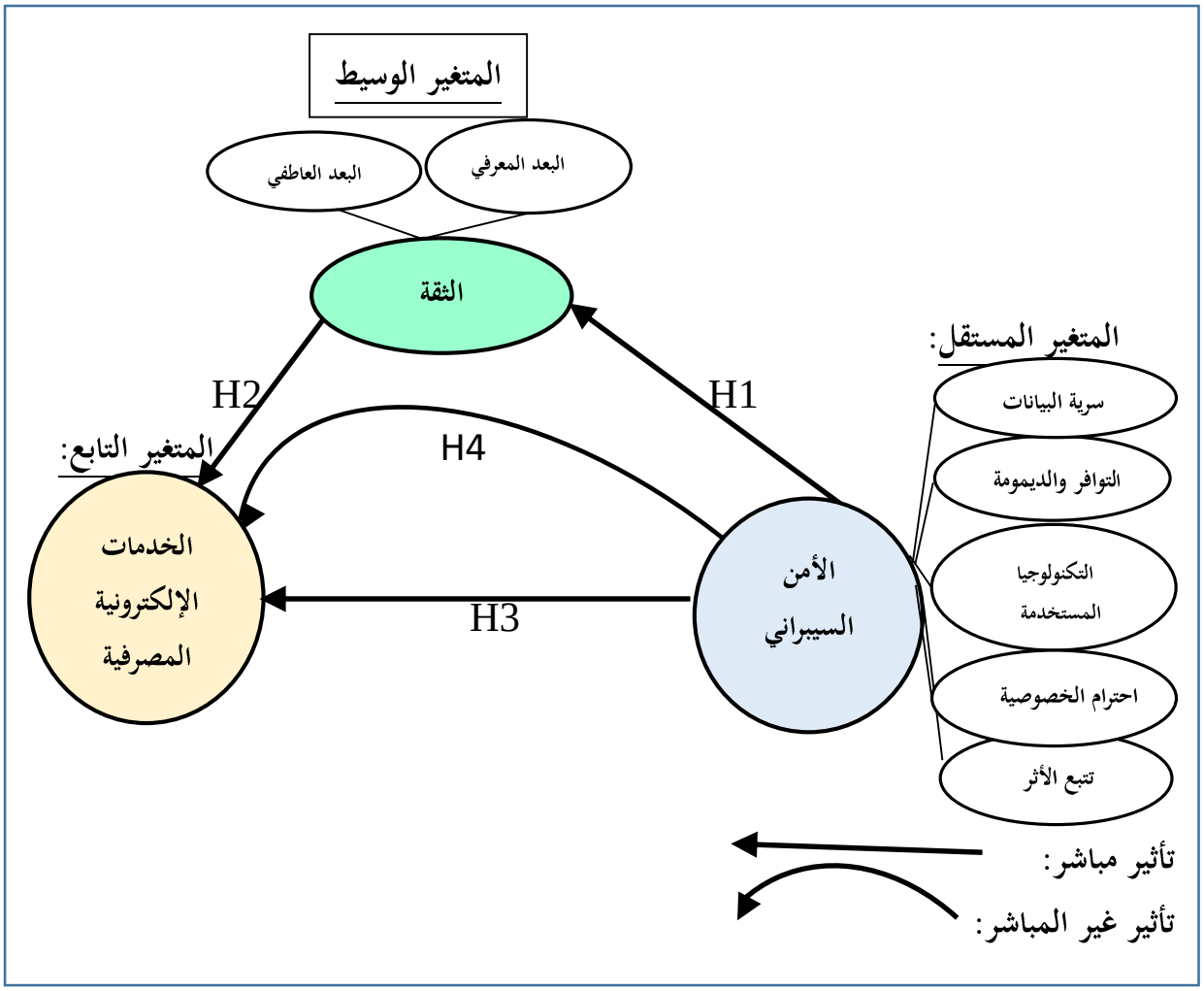
تطرقت الدراسة الحالية في جانبها النظري إلى المفاهيم الحديثة للأمن السيبراني، ثقة العملاء، الخدمات الإلكترونية المصرفية مع محاولة التعمق فيها، مع اسقاط ذلك في الجانب التطبيقي من خلال عرض مفصل حول واقع الأمن السيبراني بالبنك محل الدراسة بالجزائر من خلال توضيح سياسته المنتهجة لتحقيقه ومختلف وسائل الحماية السيبرانية المتوفرة به، إضافة إلى ذلك تم التطرق إلى الجانب التشريعي والقانوني ومختلف التعديلات المحينة والجديدة فيما يخص قانون مكافحة الجرائم الإلكترونية أو الجرائم الماسة بالمعالجة الآلية للمعطيات بالجزائر، حيث أنه لا توجد دراسة بالجزائر جمعت بين متغيرات الدراسة الثلاثة بمتغير ثقة العملاء ببعديه (البعد لمعرفي والبعد العاطفي) مع تطبيقها في المجال المصرفي وبهذا فهي تعد الأولى في بيئته، بالإضافة إلى الاعتماد في بناء الدراسة الميدانية على نمذجة المعادلات الهيكلية القائمة على المربعات الصغرى (SEM-PLS) باستخدام البرنامج الإحصائي (SMART PLS.V26).

ومن هذا المنطلق، فإن الطالب يؤكد أهمية الدراسة في البيئة المحلية، لسد الفجوة ما بين واقعنا وواقع الدول الرائدة تكنولوجيا، ما يدفعنا للاستمرار في هذا النوع من الدراسات في مختلف القطاعات التي تعتبر نقطة انطلاق ضرورية نحو تبني تكنولوجيا المعلومات وتوظيفها بشكل أمثل داخل مؤسساتنا وقطاعاتنا الحيوية.

متغيرات الدراسة:

- **المتغير المستقل: الأمن السيبراني** والمكوّن مما يلي:
  - سرية البيانات (Confidentiality).
  - التوافر والديمومة (Availability).
  - التكنولوجيا المستخدمة (Technology Used).
  - احترام الخصوصية (Privacy).
  - تتبع الأثر (Traceability).
- **المتغير الوسيطي: ثقة العملاء** والمكوّنة مما يلي:
  - البعد المعرفي (Cognitive Dimension).
  - البعد العاطفي (Emotional Dimension).
- **المتغير التابع: الخدمات الإلكترونية المصرفية.**

الشكل رقم (I): أنموذج الدراسة الافتراضي



المصدر: من إعداد الطالب بالاعتماد على بعض الدراسات السابقة.

صعوبات الدراسة:

لا تكاد تخلو أي دراسة أكاديمية من صعوبات، حيث واجهتنا الصعوبات التالية:

-قلة الدراسات السابقة المكتوبة باللغة العربية والتي تربط بين جميع متغيرات الدراسة، والمتمثلة في الأمن السيبراني للبيانات، ثقة العملاء، والخدمات الإلكترونية المصرفية، خاصة في المجال الاقتصادي عامة وتسويق الخدمات خاصة، حيث صادفنا عدة بحوث ودراسات بالنسبة لمتغير الأمن السيبراني لكنها تتحدث عن الجانب التقني البحت أو الجانب القانوني.

-التزام موظفي البنك بمبدأ السرية في بعض الجوانب الدقيقة من البحث، نظرا لنوعية المعلومات المتعلقة بأمن البنى التحتية الإلكترونية.

-احتواء الموضوع على العديد من المصطلحات والمعلومات التقنية نظرا لارتباطه الوثيق بتكنولوجيا المعلومات والاتصال، وهو ما يستلزم جهدا إضافيا من أجل فهمها وتبسيطها للقارئ.

تقسيمات الدراسة: من أجل الالمام بموضوع الدراسة وتغطية مختلف جوانبه، تم تقسيم هذا البحث إلى قسمين بحيث كل قسم يحتوي على فصلين، القسم الأول يتحدث عن الإطار النظري للأمن السيبراني، ثقة العملاء، الخدمات الإلكترونية المصرفية، والقسم الثاني يتحدث عن الدراسة الميدانية لدى عينة عملاء بنك التنمية المحلية غرداية، أما بالنسبة لمحتويات الفصول هي على النحو التالي:

الفصل الأول: يتضمن الإطار المفاهيمي للأمن السيبراني للبيانات، ويضم ثلاثة مباحث:

المبحث الأول: يتعلق بماهية الأمن السيبراني، حيث يحتوي على خمسة مطالب موزعة كما يلي: المطلب الأول يتحدث عن تعريف الأمن السيبراني، والمطلب الثاني يبين الفرق بين الأمن السيبراني والأمن المعلوماتي والأمن الإلكتروني، والمطلب الثالث يحتوي على أهداف الأمن السيبراني وخصائصه، والمطلب الرابع يتضمن مستويات الأمن السيبراني، أما بالنسبة للمطلب الخامس فهو يتطرق إلى أبعاد الأمن السيبراني.

المبحث الثاني: خصص لمفهوم البيانات الشخصية، حيث تم تقسيمه إلى خمسة مطالب موزعة كما يلي: المطلب الأول يتحدث عن تعريف البيانات الشخصية، والمطلب الثاني يبين العلاقة بين البيانات والمعلومات والفرق بينهما، والمطلب الثالث يحتوي على الرقابة على أمن بيانات العملاء في المصارف الإلكترونية، والمطلب الرابع يتضمن آلية التخزين السحابي لبيانات العملاء في البنوك الإلكترونية، أما بالنسبة للمطلب الخامس فهو يتطرق إلى أنواع التهديدات السيبرانية الماسة بأمن بيانات العملاء.

المبحث الثالث: يتناول إستراتيجية الأمن السيبراني ووسائل حماية البيانات من مخاطر الفضاء السيبراني، حيث تم تقسيمه هو الآخر إلى خمسة مطالب موزعة كما يلي: المطلب الأول يتحدث عن محاور إستراتيجية الأمن السيبراني، والمطلب الثاني يبين الوسائل التقنية لحماية البيانات في الفضاء السيبراني، والمطلب الثالث يحتوي

على الوسائل القانونية لحماية البيانات في الفضاء السيبراني، والمطلب الرابع يتضمن الوسائل البشرية لحماية البيانات في الفضاء السيبراني، أما بالنسبة للمطلب الخامس فهو يتطرق إلى المواصفة القياسية الدولية ISO 27032 لإدارة أنظمة الأمن السيبراني وآليات تعزيزه في المصارف الإلكترونية.

الفصل الثاني: خصص للحديث عن الثقة في الخدمات الإلكترونية المصرفية، وتم تقسيمه إلى ثلاثة مباحث:

المبحث الأول: يتعلق بماهية ثقة العملاء، حيث يحتوي على خمسة مطالب موزعة كما يلي: المطلب الأول يتحدث عن تعريف الثقة، والمطلب الثاني يبين الثقة العادية والثقة الرقمية، والمطلب الثالث يحتوي على خصائص الثقة وأهميتها في الخدمات الإلكترونية المصرفية، والمطلب الرابع يتضمن أبعاد الثقة ومؤشرات وأدوات قياسها، أما بالنسبة للمطلب الخامس فهو يتطرق إلى مراحل بناء ثقة العملاء وطرق تعزيزها.

المبحث الثاني: خصص للخدمات الإلكترونية المصرفية، حيث تم تقسيمه إلى خمسة مطالب موزعة كما يلي: المطلب الأول يتحدث عن تعريف الخدمات الإلكترونية المصرفية ودوافع ظهورها، والمطلب الثاني يبين أهمية ومزايا الخدمات الإلكترونية المصرفية، والمطلب الثالث يحتوي على متطلبات نجاح الخدمات الإلكترونية المصرفية، والمطلب الرابع يتضمن نظام الدفع في الخدمات الإلكترونية المصرفية، أما بالنسبة للمطلب الخامس فهو يتطرق إلى أنوع الخدمات الإلكترونية المصرفية.

المبحث الثالث: يتناول ثقة العملاء في الخدمات الإلكترونية المصرفية، حيث تم تقسيمه هو الآخر إلى خمسة مطالب موزعة كما يلي: المطلب الأول يتحدث عن فجوة الثقة في الخدمات الإلكترونية المصرفية، والمطلب الثاني يبين العوامل المحددة للثقة في الخدمات الإلكترونية المصرفية، والمطلب الثالث يحتوي على كيفية تعزيز الثقة وتضييق فجوتها في الخدمات الإلكترونية المصرفية، والمطلب الرابع يتضمن توقعات الثقة في استخدام الخدمات الإلكترونية المصرفية، أما بالنسبة للمطلب الخامس فهو يتطرق إلى نتائج ثقة العملاء في استخدام الخدمات الإلكترونية المصرفية.

أما بالنسبة للفصل الثالث: فقد خصص للمنهجية المتعلقة بالجانب الميداني للدراسة، وتم تقسيمه إلى ثلاثة مباحث هي موزعة كالآتي:

المبحث الأول: يتعلق بمنهجية البحث والبنك محل الدراسة الميدانية، حيث يحتوي على خمسة مطالب موزعة كما يلي: المطلب الأول يتحدث عن المنهج المعتمد في الدراسة، والمطلب الثاني يبين مجتمع وعينة الدراسة، والمطلب الثالث يحتوي على تعريف بنك التنمية المحلية بغرداية، هيكله التنظيمي، أهدافه ومهامه، والمطلب الرابع يتضمن أنواع بطاقات الدفع الإلكترونية الموجودة ببنك التنمية المحلية بغرداية، أما بالنسبة للمطلب الخامس فهو يتطرق إلى السياسة الأمنية السيبرانية الخاصة بالمعاملات الإلكترونية على مستوى بنك التنمية المحلية غرداية.

المبحث الثاني: خصص لتصميم أداة الدراسة وأساليب جمع ومعالجة البيانات، حيث تم تقسيمه إلى خمسة مطالب موزعة كما يلي: المطلب الأول يتحدث عن الأدوات والأساليب الإحصائية المستخدمة في الدراسة، والمطلب الثاني يبين تصميم الاستبانة، والمطلب الثالث يحتوي على نموذج القياس المقترح لمتغيرات الأمن السيبراني، والمطلب الرابع يتضمن نموذج القياس المقترح لمتغيرات الثقة، أما بالنسبة للمطلب الخامس فهو يتطرق إلى نموذج القياس المقترح لمتغير الخدمات الإلكترونية المصرفية.

المبحث الثالث: يتناول اختبار أداة الدراسة والنموذج النظري العام المقترح للدراسة، حيث تم تقسيمه هو الآخر إلى خمسة مطالب موزعة كما يلي: المطلب الأول يتحدث عن سلم القياس، والمطلب الثاني يبين النموذج العام للدراسة، والمطلب الثالث يحتوي على صدق وثبات أداة الاستبانة، والمطلب الرابع يتضمن الاختبارات الأولية لأداة الدراسة، أما بالنسبة للمطلب الخامس فهو يتطرق إلى النموذج النظري (العام) المقترح لدراسة.

وفي الأخير الفصل الرابع: خصص لتحليل وتفسر النتائج المتعلقة بالجانب الميداني للدراسة، وتم تقسيمه إلى ثلاثة مباحث كما يلي:

المبحث الأول: يتعلق بعرض وتحليل نتائج الخصائص العامة المرتبطة بالاستبيان الموجه للعملاء، حيث يحتوي على خمسة مطالب موزعة كما يلي: في المطلب الأول تم عرض وتحليل النتائج المتعلقة بالجنس، وفي المطلب الثاني تم عرض وتحليل النتائج المتعلقة بالعمر، وفي المطلب الثالث تم عرض وتحليل النتائج المتعلقة بالمستوى التعليمي، وفي المطلب الرابع تم عرض وتحليل النتائج المتعلقة بالمهنة، أما بالنسبة للمطلب الخامس عرضنا فيه وحللنا النتائج المتعلقة بالدخل.

المبحث الثاني: خصص لعرض وتحليل نتائج أبعاد الدراسة، حيث تم تقسيمه إلى ثلاثة مطالب موزعة كما يلي: في المطلب الأول تم عرض وتحليل نتائج أبعاد المتغير المستقل، وفي المطلب الثاني تم عرض وتحليل نتائج أبعاد المتغير الوسيطي، وفي المطلب الثالث تم عرض وتحليل نتائج أبعاد المتغير التابع.

المبحث الثالث: يتناول اختبار الفرضيات وتحليل مسارات العلاقات للنموذج العام للدراسة، حيث تم تقسيمه هو الآخر إلى ثلاثة مطالب موزعة كما يلي: في المطلب الأول تم اختبار وتحليل مسار الفرضيات للأثر المباشر بين متغيرات الدراسة، وفي المطلب الثاني تم اختبار وتحليل مسار الفرضيات للأثر غير المباشر بين متغيرات الدراسة، أما في المطلب الثالث تم إجراء تعديلات النموذج النهائي المقترح للدراسة والعلاقات المقترحة.

وتمت خاتمة البحث باستنتاج مجموعة من الاستنتاجات اعتمادا على الدراسة الميدانية، ليتم اقتراح بعض الاقتراحات بما يتناسب وأهداف الدراسة وفتح أسئلة معرفية قد تدخل في آفاق اهتمامات الباحثين مستقبلا.

القسم الأول

الإطار النظري للأمن السيبراني، ثقة العملاء، الخدمات الإلكترونية المصرفية

الفصل الأول

الإطار المفاهيمي للأمن السيبراني للبيانات

تمهيد:

هناك اعتمادية متزايدة على حلول تكنولوجيا المعلومات يوما بعد يوم في تسيير العمليات التجارية للمنشآت الخاصة والعامة، بل تعدى الأمر ذلك إلى المستوى الشخصي، فأصبح كثير من الأفراد يمتلك جهاز خاص به (محمولا أو مكتبيا أو يدويا) يتصفح به شبكة الإنترنت ويؤدي أعماله المختلفة، ما أدى إلى تسارع وتيرة الاستفادة من الخدمات الإلكترونية المختلفة، نظرا لما توفره من جهد ووقت وعدة امتيازات مقارنة بالماضي.

ولو أن هاته الخدمات الإلكترونية خالية من التهديدات وآمنة طوال الوقت لكان الأمر في منتهى الروعة، ولزاد التوسع في تقديم المزيد منها بكل سهولة في شتى المجالات، لكن ما يحدث هو أن تلك الخدمات الإلكترونية هي تتعامل مع معلومات وبيانات حساسة وبالغة الأهمية، وفي نفس هي معرضة لكثير من المخاطر والتهديدات، بل أثبتت الدراسات الحديثة اختراق كثير من تلك الأنظمة أو حتى تعطيلها والتعدي على معلومات وبيانات عملائها، مثلما حصل في عدة بنوك عبر العالم.

إذا فالأمن السيبراني ضرورة ملحة وليس حلا اختياريا، بل يمكن القول أن أي منشأة تتضمن شبكة اتصال وموارد تقنية لا بد أن يرافقها مشروع توأم للأمن السيبراني بما يشمل من تجهيزات لازمة لحماية البيانات التي يجري التعامل معها ومعالجتها.

من خلال هذا الطرح، ارتأينا أن تتعلق الأدبيات النظرية للفصل الأول بمفاهيم الأمن السيبراني للبيانات في مجال الخدمات الإلكترونية المصرفية، عليه تم تقسيم الفصل إلى ثلاثة مباحث كما يلي:

- المبحث الأول: ماهية الأمن السيبراني.
- المبحث الثاني: مفهوم البيانات الشخصية.
- المبحث الثالث: إستراتيجية الأمن السيبراني ووسائل حماية البيانات من مخاطر الفضاء السيبراني.

المبحث الأول: ماهية الأمن السيبراني (Cyber Security)

تُعتبر مهمة تحديد المصطلحات في جميع التخصصات وشتى الدراسات أول تحد يُواجهه المفكرون ويتعرض له الباحثون، نظرا لما تطرحه من إشكاليات تجعل من الصعوبة الاتفاق على تعريفات واضحة وموحدة، حيث يمكن تعميمها على جميع الحقول المعرفية، إذ يعتبر مصطلح الأمن السيبراني واحدا من هذه المصطلحات التي عرفت تعددا في التعريفات المقدمة له.

المطلب الأول: تعريف الأمن السيبراني

من خلال ما سبق، ذكرنا أن مصطلح الأمن السيبراني Cyber Security عرف تعددا في التعريفات المقدمة له، فمصطلح سيبار Cyber هو لفظ أصله اليونان، مشتق من كلمة Kybernete، معناها القيادة أو التحكم، من مصدر كلمة Cybernetics والتي تعني: "علم الاتصالات وأنظمة التحكم الآلي في كل من الآلات والأشياء الحية".[1]

كما قدمت **وزارة الدفاع للولايات المتحدة الأمريكية "البنتاغون"** تعريفا لمصطلح الأمن السيبراني، فاعتبرته: "جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية والإلكترونية من مختلف الهجمات، التخريب، التجسس والحوادث".[2]

في حين **الإعلان الأوروبي** اعتبر الأمن السيبراني أنه: "قدرة النظام المعلوماتي على مقاومة محاولات الاختراق أو الحوادث غير المتوقعة التي تستهدف البيانات".[3]

وفي عام 2011 صدر تقرير عن **الاتحاد الدولي للاتصالات (ITU)** يُعرف من خلاله الأمن السيبراني بأنه: "مجموعة من المهمات، تتمثل في تجميع وسائل، وسياسات، وإجراءات أمنية، ومقاربات لإدارة المخاطر، ومبادئ توجيهية، وتدريبات، وممارسات فضلى، وتقنيات، يمكن استخدامها لحماية البيئة السيبرانية، ومُوجدات المؤسسات والمستخدمين".[4]

أما عن بعض فقهاء المركز العربي للبحوث القانونية والقضائية، فقد عرَفوا الأمن السيبراني على أنه: " أمن الشبكات والأنظمة المعلوماتية والبيانات والمعلومات والأجهزة المتصلة بالإنترنت، فهو المجال الذي يتعلق بإجراءات ومقاييس ومعايير الحماية المفروض اتخاذها، أو الالتزام بها لمواجهة التهديدات ومنع التعديات، أو

---

[1] Joanna Defranco, **What Every Should Know About Cyber Security and Digital Forensics**, Boka Ranton: CRC press, 2014, p40.

[2] Daniel Ventre, **Cyberattaque et cyber défense**, La Voisier, Paris, 2011, P 103.

[3] Douwe Korff, **Cyber Security Definitions** – a selection, in: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CPDP%202015%20-%20KORFF%20Handout.pdf, Retrieved: 03-01-2022, 22:45.

[4] تقرير صادر عن الاتحاد الدولي للاتصالات، التابع للأمم المتحدة عام 2011، الموقع: (http://www.itu.int)، تاريخ الاطلاع: 28-07-2022، الساعة: 10:40.

للحد من آثارها في أقصى وأسوأ الأحوال، حيث يرتبط هذا الأمن ارتباطا وثيقا بأمن البيانات والمعلومات. فالوصول إلى هذه الأخيرة أو بثها، وكذا الاطلاع عليها أو المتاجرة بها، أو تشويهها أو استغلالها، هو ما يقف وراء عمليات الاعتداء على الشبكات والإنترنت في غالب الأحيان".[1]

وهذا ما ذهب إليه كل من: Neittaanmaki Pekka, Lehto Martti في كتابهما المعروف بعنوان: "Cyber Security: Analytics, Technology and Automation"، حيث اعتبرا أن الأمن السيبراني هو: "عبارة عن مجموعة من الإجراءات التي تُتخذ في الدفاع ضد هجمات قراصنة الكمبيوتر وعواقبها، ويتضمن تنفيذ التدابير المضادة المطلوبة". كما عرفه إدوارد أمورسو Amoroso Edward بأنه: "مجموعة وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، حيث تشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة، وكشف الفيروسات ووقفها، وتوفير الاتصالات المشفرة".[2]

وقد عرفه آخرون بأنه: "عبارة عن مجموع الوسائل التقنية والإدارية التي يتم القيام بها لمنع الاستخدام غير المشروع، وكذا سوء استغلال المعلومات الإلكترونية ونظم الاتصالات والبيانات التي تحتويها، بهدف ضمان توافر واستمرارية عمل النُظم، وكذا تأمين حماية سرية وخصوصية البيانات الشخصية، وحماية المستخدمين من المخاطر في الفضاء السيبراني".[3]

بينما قدم **المشرع الجزائري** تعريفا للأمن السيبراني على أنه: "مجموع الأدوات والسياسات، ومفاهيم الأمن والآليات الأمنية، والمبادئ التوجيهية، وطرق تسيير المخاطر، والأعمال والتكوين، والممارسات الجيدة والضمانات، والتكنولوجيات التي يمكن استخدامها في حماية الاتصالات الإلكترونية، ضد أي حدث من شأنه المساس بتوفر وسلامة وسرّية البيانات المخزنة أو المعالجة أو المرسلة".[4]

لما سبق ذكره، ومن خلال التعاريف السابقة يمكن أن نستنتج أن:

- الأمن السيبراني هو النشاط أو الخدمة التي تُؤمّن وتحمي الموارد المرتبطة بتقنية المعلومات والاتصال.
- الأمن السيبراني يحدُ من الأضرار المادية والخسائر المالية التي تنتُج في حال وقوع المخاطر والتهديدات أو الاعتداءات في الفضاء السيبراني.

---

[1] Ramjee Prasad, Vandana Rohokale, **Cyber Security**: **The Lifeline of Information and Communication Technology**, published by springer, India, 2019, p 3.

[2] Neittaanmaki Pekka, Lehto Martti, **Cyber Security**: **Analytics**, **Technology and Automation**, Switzerland: Springer international Publishing, 2015, p 25.

[3] Kaushik Kumar Panigrahi, **Information Security and Cyber Law**, Published by Tutorials Point, India, 2015, p1.

[4] قانون رقم: 18-04، المتعلق **بالقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية**، المؤرخ في: 24 شعبان 1439 الموافقـ 10ماي 2018، المادة 10، ج.ر.ج.ج، الباب الأول، القسم الثاني، العدد 27، الصادر بتاريخ: 13 ماي 2018، ص 7.

- بعد وقوع الحادثة الأمن السيبراني يُعيد الوضع إلى ما كان عليه بأسرع وقت ممكن.
- الأمن السيبراني غايته عدم توقف المنشأة عن العملية الإنتاجية مهما كان الوضع.

المطلب الثاني: أهداف الأمن السيبراني وخصائصه

انطلاقا مما سبق، فإن للأمن السيبراني عدة أهداف مختلفة أساسها القدرة على مقاومة مختلف المخاطر والتهديدات المتعمدة وغير المتعمدة وكذا الاستجابة والتعافي، من خلال الاعتماد على مجموعة من الخصائص وبالتالي التحرر من الأخطار أو الأضرار الناجمة عن تعطيل أو إتلاف تكنولوجيا المعلومات والاتصالات، أو بسبب سوء استخدام تكنولوجيا المعلومات والاتصالات، ومن أهدافه الأخرى التي يسعى لتحقيقها ما يلي:

❖ **أهداف الأمن السيبراني:**

- الحفاظ على سرية المعلومات من خلال قصر النفاذ على الجهات المصرح لها فقط، (بدون نفاذ غير مشروع).
- الحفاظ على دقة وسلامة البيانات والبرامج وعدم فساد حالتها، أي (بدون معلومات زائفة وبدون أخطاء).
- الحفاظ على توافر تقديم الخدمات بشكل مستمر وبدون انقطاع أو تدهور، أي (بدون تأخير أو حجب).
- الحفاظ على البيانات والبرامج للفترة المطلوبة، أي طول العمر (بدون تدمير نهائي).
- ضمان الأصل والمنبع والجهة والصدق في كل التصرفات، بمعنى (عدم الإنكار) والقدرة على الاستدلال على الفاعل من خلال تتبع الأثر (بدون نزاعات نظرا لحجة الدليل).
- احترام الخصوصية الرقمية للمستخدمين والمتعاملين الإلكترونيين.
- الاستيقان والتأكد، بمعنى (بدون شك يكتنف هوية المورد).
- الوصول إلى الوضع الأمثل لأداء نظام المعلومات جنبا إلى جنب مع مستوى أداء الأمن المطلوب.[1]
- خلق الثقة في التطبيقات والخدمات المقدمة خاصة في المعاملات التجارية والمالية إلكترونيا.
- تطوير السياسات والإجراءات الأمنية اللازمة للمؤسسات والدول ونمو اقتصادها.
- تعزيز حماية أنظمة التقنيات التشغيلية على كافة الأصعدة، وما تقدمه من خدمات وما تحويه من بيانات.
- التصدي لهجمات وحوادث أمن المعلومات التي تستهدف مؤسسات القطاع العام والخاص.
- توفير بيئة آمنة وموثوقة للتعاملات في مجتمع المعلومات.
- التخلص من نقاط الضعف في أنظمة الحاسب الآلي والأجهزة المحمولة باختلاف أنواعها.
- سد الثغرات في أنظمة المعلومات.
- اتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين على حد سواء، من التهديدات والمخاطر المحتملة في مجالات استخدام الإنترنت.

[1] الاتحاد الدولي للاتصالات (ITU)، **دليل الأمن السيبراني للبلدان النامية**، طبع في جنيف سويسرا، 2006، ص 101.

- تدريب الأفراد على آليات وإجراءات جديدة لمجابهة التحديات الخاصة باختراق أجهزتهم التقنية بغية الضرر بمعلوماتهم الشخصية سواء بالإتلاف أو السرقة.[1]

❖ **خصائص الأمن السيبراني:**

يتميز الأمن السيبراني بعدة سمات أهمها:[2]

-الأمن السيبراني ليس مسار عمل لمرة واحدة، إنما هو عملية مستمرة مرافقة كونه يحتوي على آليات دفاع مبتكرة لمواجهة المخاطر والتهديدات التي تقع على الأنظمة والشبكات وغيرها.

-يعمل على خلق نظام بيئي سيبراني آمن ونظام موثوق به.

-يقوم بعملية وقائية رقابية مُسبقة بُغية البحث عن المخاطر والتهديدات، والعمل على حلها وسد مختلف الثغرات.

-يعمل على الدفاع اللاحق (البعدي)، الذي يتمثل في قاعدة إرجاع الوضع إلى ما كان عليه سابقا.

-يوفر خاصية التنبيه إلى وجود خطأ أو إساءة استخدام الشبكات التي تُعرَض البيانات والمعلومات إلى الخطر من داخل المؤسسات.

-يقوم الأمن السيبراني بتغطية المخاطر الخارجية ومراقبة التهديدات المختلفة.

المطلب الثالث: مستويات الأمن السيبراني (Cyber Security Levels)

من المهم التعرف على مستويات الأمن السيبراني، والتي تقسم الى ثلاثة أقسام: الأول على المستوى الدولاتي، والثاني على المستوى المؤسساتي، أما الثالث على المستوى الفردي:[3]

1-على المستوى الدولاتي (Contry): بما أن الدولة هي الفاعل المحوري في تسيير الفضاء الافتراضي انطلاقا من إمكاناتها المادية والتقنية والبنيوية والبشرية والقانونية والتنظيمية، نشير هنا أساسا إلى الاحتكار القانوني والمُنظم للدولة للفضاء الافتراضي، الذي يتم من خلال مختلف أجهزتها.

2-على المستوى المؤسساتي (Institutional): تمتلك بعض المؤسسات والشركات الكبرى التكنولوجيا وموارد قوية تفوق قدرة بعض الدول، ولا تنقصها سوى شرعية ممارسة هاته القوة التي ما زالت حكرا على الدول، مثلا خوادم شركات مثل جوجل (Google)، ومايكروسوفت (Microsoft)، وفايسبوك (Facebook)،

---

[1] مني عبد الله السمحان، **متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود**، مجلة كلية التربية، جامعة المنصورة، العدد 11، جويلية 2020، ص 12.

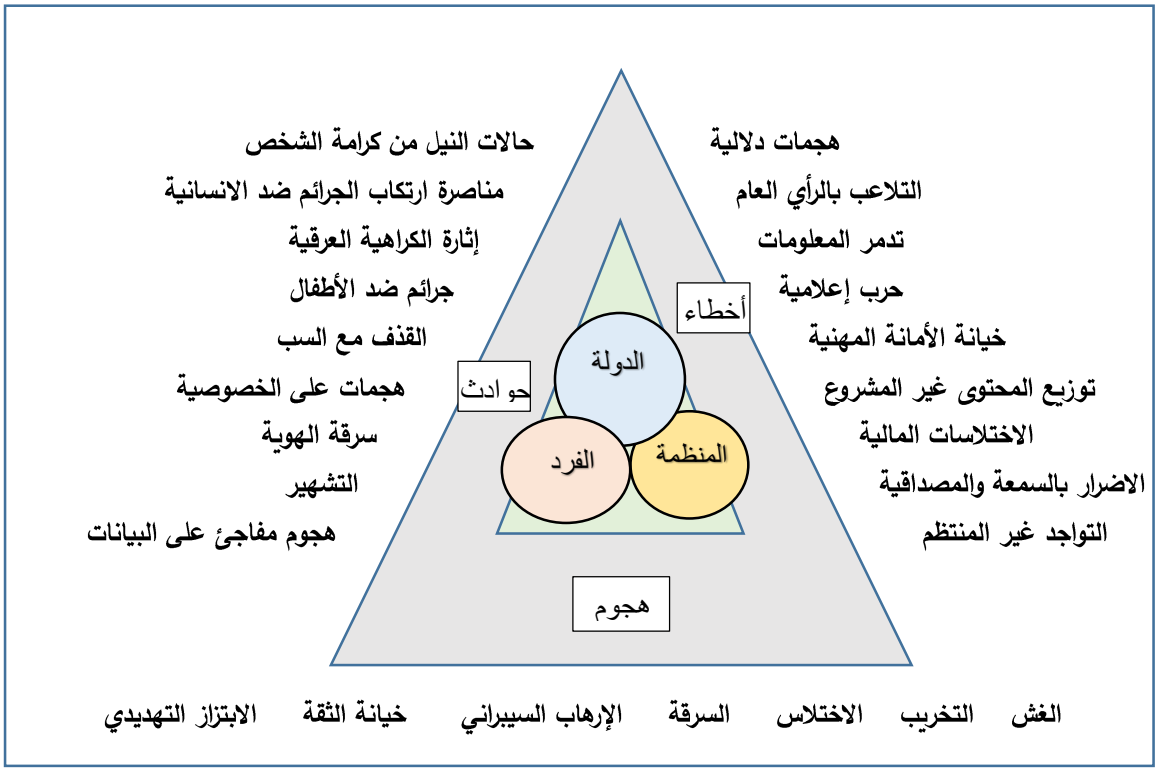
[2] خالد ظاهر عبد الله جابر السهيل المطيري، **دور التشريعات الجزائية في حماية الأمن السيبراني بدول مجلس التعاون الخليجي**، مجلة البحوث الفقهية والقانونية، العدد 28، يوليو 2022، ص 1006.

[3] محمد محمود العمري، **مدخل إلى الأمن السيبراني**، دار زهران للنشر والتوزيع، عمان، الأردن، 2020، ص 33.

التي تسمح لها بامتلاك قواعد البيانات الضخمة أو العملاقة التي من خلالها تستكشف وتستغل مختلف الأسواق، وكذا تؤثر في اقتصاديات الدولة وفي ثقافة المجتمعات أو حتى توجهاتها.

3-على المستوى الفردي (Singles): أصبح الفرد بفضل الفضاء السيبراني فاعلا مؤثرا في العلاقات الدولية وله القدرة والامكانية على إحداث الثورة الرقمية، حيث تُصبح هذه الثورة مجال استخدام للدولة نفسها، ومثال على ذلك ما قام به المبرمج المواطن الأمريكي مارك زوكربيرغ (Mark Zoukerberg) سنة 2004 م، حين أسس مع زملائه شبكة عالمية تسمى (فايسبوك) التي استقطبت أكثر من مليار مستخدم عبر العالم وأصبحت أكبر موقع اجتماعي في العالم.

الشكل رقم (I-1): مستويات الأمن السيبراني وما يحيط به



المصدر: الاتحاد الدولي للاتصالات (ITU)، دليل الأمن السيبراني للبلدان النامية، جنيف سويسرا، 2006، ص 8.

يوضح الشكل أعلاه رقم (I-1): أن للأمن السيبراني ثلاثة مستويات، متدرجة من المستوى الأدنى إلى المستوى الأعلى، انطلاقا من أمن الفرد إلى أمن المنظمة وصولا إلى أمن الدولة، حيث أن هناك تهديدات ومخاطر متزايدة تخلفها استخدامات التكنولوجيا الحديثة خاصة تلك المرتبطة باستعمال الإنترنت، إذ تحيط بتلك المستويات كما هي واضحة في الشكل، فموضوعنا اليوم يتحدث عن الأمن السيبراني المتعلق بالعملاء (الأفراد) يعني المستوى الأول في المثلث، وما يحيط به من مجموعة مخاطر وتهديدات لها آثار سلبية وخيمة مثل: (تدمير المعلومات والبيانات، التخريب، سرقة، انتحال الهوية، التشهير، الاختلاس المالي، الغش، توزيع المحتوى

غير المشروع، خيانة الثقة...الخ). وبهذا قد بات من الضروري وجود حلول جاهزة على المستوى الفرد بدرجة أولى والمنظمة بدرجة ثانية والدولة بدرجة ثالثة، هاته الحلول تقنية، وتنظيمية، وقانونية، وإدارية، وتثقيفية، وتوعوية، أو بالأحرى ما يتوافق واعتماد سياسة أمنية شاملة ومتكاملة تضع مسألة توفير الأمن السيبراني على رأس الأولويات والاستراتيجيات، وتعزز بناء الثقة في الفضاء السيبراني، وتولد النمو الاقتصادي المرغوب فيه، الذي يفيد الفرد خاصة والمجتمع كافة.

المطلب الرابع: أبعاد الأمن السيبراني

يمكننا تعريف أبعاد الأمن السيبراني للبيانات، أنها مجموعة العناصر الواجب توافرها لحماية هاته البيانات، بحيث يُغطي كل عنصر من هذه العناصر جانبا من جوانب الحماية المطلوبة، وبهذا تتكامل هذه العناصر حتى توفر الحماية وفي حال فقد أي منها سيؤدي ذلك إلى خلل أمني، وللمحافظة على أمن البيانات في التطبيق أو النظام يجب أن تتوفر خمسة عناصر هي:[1]

1-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 إليها إلا من الأشخاص المصرح لهم فقط.

وتعني أيضا الحفاظ على المعلومات والبيانات من أن يُطلع عليها (قراءتها وفهمها) غير الأشخاص المصرح لهم، أو بعبارة أخرى الكشف غير المصرح به، فعند إرسال رسالة سرية فإن ذلك يتطلب ألا يراها إلا المرسل والمرسل إليه، لكن إن استطاع أحد الاطلاع عليها فإنه لا يستطيع أن يفهم محتواها، بمعنى يجب أن تكون غير مفهومة، وكذا تضمن السرية بوجود مستوى الحماية المطلوب في كل مكوَن من مكونات معالجة البيانات والمعلومات، كما يجب أن يتوافر هذا المستوى من الحماية في كل مراحل المعالجة ليشمل البيانات والمعلومات المخزنة، والبيانات والمعلومات المرسلة، وكذا تلك التي وصلت إلى وجهتها النهائية، لذلك يجب أن تشمل السرية حماية سيل البيانات من التحليل أثناء النقل (من قبل من يحاول كسر سريتها)، فعندما تكون البيانات مشفرة مثلا، فإن ذلك يصَعب من مهمة المتطفل بغرض فك شفرتها، إن لم يجعل ذلك مستحيلا (قياسا على الوقت المتاح).

[1] منى الأشقر جبور، محمود جبور، **البيانات الشخصية والقوانين العربية**، دراسات وأبحاث المركز العربي للبحوث القانونية والقضائية (الأمن المعلوماتي والأمن القانوني)، بيروت، لبنان، 2019، ص 18.

كما أن هناك العديد من الطرق لتوفير عنصر السرية، هي تتراوح بين حجب المعلومة يدويا وعدم تسليمها إلا للأشخاص المرح لهم، إلى طرق التشفير الجديدة أو الحديثة التي تعتمد على خوارزميات رياضية معقدة يصعب فكّها، إن لم يكن ذلك مستحيلا، من هنا يمكننا القول أنه يمكن توفير عنصر السرية من خلال تشفير البيانات سواء الثابتة أو المنقولة مع تطبيق سياسة صارمة بخصوص التحكم بالوصول، وكذا تصنيف المعلومات وتدريب العاملين على الأنظمة وسياسات الأمن السيبراني تدريبا جيدا.

قد يتبادر إلى ذهن البعض أنه عندما يتوافر عنصر السرية فإنه بذلك يصبح المعلومات والبيانات آمنة، أو بعبارة أخرى أن التشفير كوسيلة لتحقيق عنصر السرية يضمن أمنها بشكل كامل وهذا مفهوم خاطئ، أما الصحيح فالسرية ما هي إلا عنصر واحد من مجموعة عناصر يجب توفرها جميعا لتصبح البيانات والمعلومات آمنة، فتوفر عنصر السرية لا يضمن كشف تعديل البيانات بعد النقل أو التحويل مثلا، فقد يتم تغيير بيانات معينة في الرسالة المشفرة وعندما يفك المستقبل شيفرة هذه الرسالة يحصل على بيانات مقبولة ظاهريا له، لكنها غير البيانات الحقيقية، وكذلك فإن توفر عنصر السرية لا يغني عن عنصر التحقق من الهوية وعنصر عدم الإنكار.

ومن الأمثلة على الخروقات والتطفلات الممكنة لأمن المعلومات التي تتم في حال عدم توافر عنصر "السرية"، هي إمكانية الاطلاع على معلومات مهمة وحساسة من قبل أي شخص إذا وُضعت هذه المعلومات وسط تخزين خارجي وهي غير مشفرة بسبب حاجة ما، فتصبح هذه المعلومات خارج المنظومة الأمنية للمنشأة، وبهذا لا يحميها لا تحقق من الهوية ولا تحكم بالوصول، لذا يجب أن تكن مشفرة، وفي المثال الآخر المتعلق بإرسال مرفق عبر البريد الإلكتروني العام (Google أو Hotmail) وهو غير مشفر ويحتوي على معلومات مهمة جدا، ففي هذه الحالة البريد الإلكتروني والمرفقات التي معه هي معرضة للاطلاع عليها من قبل أي شخص بما فيهم الشركة المقدمة لخدمة البريد، ومن الأمثلة المشهورة على خروقات أخرى، حفظ ملف النسخ الاحتياطي في وسط خارج المنشأة، لكنه غير مشفر، ففي هذه الحالة هو عرضة للاطلاع عليه من قبل الآخرين، وكذلك بالنسبة الحال فيما يتعلق بالمعلومات والبيانات المرسلة عبر دوائر الاتصالات الخارجية للشبكات الواسعة WAN) إذا لم تكن هي الأخرى مشفرة.

2-التوافر والديمومة (Availability):

يُقصد بتوافر المعلومة، أن تكون قابلة للوصول إليها قصد استخدامها حين الطلب عليها من قبل أي شخص أو أي جهة محددة ومعروفة، وفي أي وقت مصرح به، ويمكن القول أن خدمة التوافر هي تلك الخدمة التي تحمي النظام ليبقى دائما متاح، ومن هنا يُطلق عليها أحيانا بالديمومة، وهي موجهة خصيصا إلى أي هجوم أو خلل يمكن أن يؤدي إلى عدم توافر الخدمات أو انقطاعها وتعطلها، ومن المثال على ذلك هجوم الفيروسات، وهجمات حجب الخدمة أو منعها أو تعطيلها (Denial of Service-DoS)، إذ يتطلب هذا التحدي في غالب الأحيان الحماية المادية والتقنية، كتقنيات توفير نظم احتياطية للمعلومات والطاقة الكهربائية، فالهدف

العام من توفير عنصر التوافر والديمومة هو أن تكون الشبكات والأجهزة والنظم والبرامج والخدمات المختلفة متاحة في جميع الأوقات حين يحتاج إليها المستخدم، ولتأمين توافر الأنظمة والخدمات والبيانات، يجب تحديد الأحجام المناسبة لحماية اللبنية التحتية، وتوفير الإدارة التشغيلية للموارد، بمعنى الإبقاء على البيانات متوفرة للمستخدم مع إمكانية الوصول إليها في أي وقت دون تعطل ذلك بسبب خلل ما في أنظمة قواعد البيانات أو وسائل الاتصالات.

تجدر الإشارة إلى أنه يجب الموازنة بين الحماية وتوافر المعلومات، كونه إذا سُمح لأي شخص بالدخول إلى المعلومات بأي طريقة اتصال وفي أي وقت ومن أي مكان، فإننا بذلك نحصل على درجة عالية من توافر هاته المعلومة، لكن في المقابل ينتج عنه ثغرات أمنية كبيرة جدا، وإذا عكسنا ذلك فإنه إذا جرى تقييد المعلومات بشكل جيد من أجل حمايتها سيكون من الصعب توفيرها لجميع الشرائح التي تحتاجها في الأوقات المناسبة، إذا المطلوب هو الموازنة بين ذلك للوصول إلى منزلة وسطية.

ومن الأمثلة على الخروقات الماسة بأمن المعلومات والبيانات التي يمكن أن تتم في حال عدم توفر عنصر "التوافر والديمومة"، هو إمكانية تدمير أنظمة المنشأة كاملة أو جزئيا باستخدام برنامج تدمير أو فيروس تدميري حديث الإنتاج لا يوجد له برامج حماية أو تحديثات (رقع (Patches)) لأجل إلغاء فاعليته، ففي هذه الحالة إذا لم تكن هناك أنظمة احتياطية يتم استخدمها بدل التي دُمرت لأجل أن تضمن توافر المعلومة فسيكون هناك توقف تام أو جزئي في عمل المنشأة ولو لوقت محدد، كون توفير التحديثات والرقع اللازمة لإلغاء فاعلية هذه البرامج التدميرية والفيروسات هو يحتاج إلى وقت من أول ظهور لها، ولن يكون الحل إلا إذا تم إنتاج تحديثات ورقع مضادة لها وتوفيرها من قبل الجهات المنتجة لمثل هاته البرامج التطبيقية وأنظمة التشغيل.

وبهذا فإن إجراءات صيانة المعدات، وتوفير نسخ احتياطية، وترقية نظم التشغيل إلى أحدث الإصدارات، بالنسبة للبنوك هي إجراءات وقائية حتى لا يقع البنك في مشكلة انقطاع الخدمة، كما يجب اعداد العدَة لتجاوز الكوارث المحدثة من قبل الانسان كالتخريب والحرق المتعمد أو الكوارث الطبيعة كالزلازل والفيضانات.[1]

3-تتبع الأثر (Traceability):

هي الخدمة التي من خلالها يضمن عدم إنكار أي جهة أو شخص ما قام بعملية أو بتصرف متصل بالبيانات أو مواقعها[2]، على سبيل المثال: إذا منحت جهة معينة لجهة أخرى صلاحية أو مهام شراء منتج معين، ثم بعد ذلك أنكرت أنها منحت لها هذه الصلاحية، فإن خدمة عدم الإنكار تكشف ذلك بكل سهولة، أي بمعنى توفر قدرة إثبات وقوع العملية التفاعلية من خلال عملية تتبع الأثر.

---

[1] أسامة حسام الدين، **مقدمة في الأمن السيبراني 0.2**، كلية علوم وهندسة الحاسبات، أكاديمية سيسكو، 2017، ص 10.

[2] مريزق عدمان، عماد بوقلاشي، **الأمن المعلوماتي في ظل التجارة الإلكترونية، إشارة إلى حالتي تونس والجزائر**، مداخلة ضمن فعاليات الملتقى العلمي الدولي الرابع حول عصرنة نظام الدفع في البنوك الجزائرية وإشكالية اعتماد التجارة الإلكترونية في الجزائر، عرض تجارب دولية، منشورة، المركز الجامعي خميس مليانة، يومي: 26-27 أفريل 2011، ص4.

وللتوضيح أكثر، فإنه في حال إرسال رسالة بين طرفين، فالأثر التكنولوجي يُثبت إرسال المرسل لها كما يُثبت استقبال المستقبل لها، بحيث لا يمكن إنكار أي منهما ذلك، وأهمية هذا الإثبات تزداد بازدياد أهمية الرسالة نفسها، وبالإضافة إلى قدرة الاستدلال على الفاعل وإمكانية اقتفاء الأثر وقابلية المراجعة لتحديد المسؤولية، فخدمة تتبع الأثر أو خدمة عدم الإنكار هي تشمل كذلك إثبات وقوع العمليات الإلكترونية في تواريخ وأوقات معينة عن طريق إلحاق بصمة الوقت والتاريخ بالعملية نفسها (Time Stamping)، إذا قام أحد بعملية إلكترونية معينة في تاريخ ووقت معينين ثم أنكر أنه قام بها في ذلك الوقت والتاريخ، فإن ذلك سيُكشف بالرجوع إلى بصمة الوقت والتاريخ الأصلية، ويسمى هذا بقابلية التدقيق لدى النظام.

نقول الأثر، كون البيانات المعالجة إلكترونيا هي تخزن على هيئة نبضات كهربائية وتجمع في دوائر إلكترونية، أو تخزن على أسطوانات أو أشرطة ممغنطة، فيقوم الجاني بنسخها على دعامات أخرى دون أن يترك لذلك أثرا، إلا إذا تم اتخاذ إجراءات دفاعية صارمة على هذا الاستنساخ.

ومن الأمثلة على بعض الخروقات الممكنة لأمن المعلومات التي تتم في حال عدم توفر عنصر عدم الإنكار أو تتبع الأثر، إمكانية تنصل أحد الأشخاص من مسؤولية التوقيع أو التصديق على وثيقة إلكترونيا، هنا إذا لم يتوفر عنصر "عدم الإنكار/تتبع الأثر" فلا يمكن على الإطلاق إثبات أن هذا الشخص هو من قام بالتوقيع على الوثيقة.

4-التكنولوجيا المستخدمة (Technology Used):

تعني الخدمة التي من خلالها يتم الحفاظ على سلامة المعلومات والبيانات من أي تعديل، أو حذف، أو إضافة، أو توجيه، أو إعادة تركيب، وهذا الأمر جد مهم لضمان الثقة في المعلومات وأنها هي الأصلية دون زيادة أو نقصان، فقد تكون هاته المعلومات مشفرة وسريتها مضمونة، إلا أنها قد تتعرض للتغيير طالما أنها إلكترونية، لذا لا بد من إيجاد طريقة لكشف هذا التغيير، وهو ما يوفره عنصر التكنولوجيا المستخدمة من خلال دقة الأنظمة المعالجة وسلامتها من التلاعب أو التغيير غير المصرح به، كما يتطلب ذلك أن تعمل البرامج وأنظمة الشبكات والأجهزة المختلفة بانسجام تام، للمحافظة على البيانات والمعلومات ومعالجتها ونقلها إلى وجهتها المقصودة دون أي تعديل أو تغيير غير متوقع، فهذا الأمر من المفروض أن يُولد ويعزز الثقة لدى المتعاملين، وللحيلولة دون التلاعب، لا بد من وجود طريقة للتصديق على أنها لم تتعرض للتغيير أو التعديل أثناء الخزن أو النقل.

بالإضافة إلى سلامة ومتانة البنى التحتية بوجود معدات تكنولوجية حديثة وأجهزة فنية توفر الحماية التقنية ضد الأعطال والقصور في الموارد، وغالبا ما تعمل هذه المكونات بطريقة آلية دون التدخل البشري.[1]

ومن بين الأمثلة على عنصر التكنولوجيا المستخدمة، دقة الأنظمة المعالجة وسلامتها مع وجود رسائل التحذير (Alerts) تُنبئ عن حدوث مشكلة ما أو إمكانية حدوثها، بحيث تمكننا من معرفة ظروف المشكلة وتاريخها

[1] ذيب بن عايض القحطاني، **أمن المعلومات**، دار النشر لمدينة الملك بن عبد العزيز للعلوم والتقنية KACST، الرياض، السعودية، 2015، ص91-100.

مع الكشف عن عمليات الاختراقات أو التطفل أو التعطيل، مع المساعدة على استعادة الأحداث، والتغييرات المختلفة التي طرأت على الملفات، وكشف المخالفات الأمنية التي ترتكب داخل البرامج.

5-احترام الخصوصية (Privacy):

من الصعب وضع تعريف جامع وشامل للحق في الخصوصية أو الحق في الحياة الخاصة، كون تعريف هذا الحق هو يرتبط بالتقاليد والثقافات والقيم الدينية السائدة وكذا النظام السياسي في كل مجتمع، فالخصوصية تُعبر عن حق العملاء في عدم نشر أو بَث بياناتهم الشخصية المتعلقة بتعاملاتهم أو بحياتهم الخاصة كالنشاط، ومكان التواجد، والعلاقات الشخصية، أو حتى التسجيل والتنصت بالوسائل الإلكترونية، على سبيل المثال احترام الخصوصية في البنوك تتم بداية من طلب كلمة سر خاصة عند إنشاء حساب على الموقع الرئيسي للبنوك التجاري إلى غاية مختلف المعاملات الخاصة ببطاقات الدفع الإلكترونية، كما يوجد عدة حلول تكنولوجية يُجرى استخدامها لتحقيق خصوصية البيانات الشخصية.

من المفروض أن سياسة احترام الخصوصية هي تبني وتعزز ثقة العملاء في الفضاء السيبراني، ومستوى هذه الثقة يؤثر في نوعية وحجم البيانات التي يتم الحصول عليها، فالعميل لا يقدم بياناته إلى أي طرف كان، إلا من أجل الحصول على قيمة أو منفعة، حيث أن أي متجر إلكتروني هو يسعى إلى الحصول على البيانات أو المعلومات الدقيقة ذات المصداقية، ولا يتحقق هذا إلا بتحقيق الثقة لدى العملاء، إذ يعود الاهتمام بالمحافظة على الحق في الخصوصية إلى بداية استخدام تكنولوجيا المعلومات والاتصال، وانشاء قواعد البيانات الشخصية.

ومن الأمثلة على الجوانب القانونية التي تخص الاعتداء على حق الخصوصية، في عدد من الجرائم والأعمال غير المشروعة منها: الاتجار بالبيانات الشخصية كأسماء الأشخاص وعناوينهم، وأرقام حساباتهم المصرفية أو الائتمانية، التشهير، انتحال هوية الأشخاص، انتحال الصفات، اختراق أنظمة المعلومات، الابتزاز، الوصول إلى الأسرار التجارية أو المهنية، المراقبة أو التتبع والرصد غير المشروع لحركة الأشخاص وأموالهم، التمييز العنصري أو الديني، وكذا تكوين ملفات معلومات دون سبب شرعي...إلخ.[1]

بناء على مجموعة من الدراسات السابقة العربية منها والأجنبية، اعتمد الطالب في دراسة الأمن السيبراني ومعرفة مكوناته وأبعاده خاصة منها ذات الطرح الاقتصادي، استنادا إلى مؤشرات مقياس كل من: (Kritika Law، 2007)[2]، (علوطي لمين، 2009)[3]، (بربار، قلمين، 2014)[4]،

---

[1] سعيد زيوش، **التجارة الإلكترونية وآليات حماية خصوصية المستهلك الجزائري**، مجلة هيرودوت للعلوم الإنسانية والاجتماعية، بريكة، باتنة، الجزائر، المجلد 7، العدد 25، 2023، ص 10.

[2] Kritika Law, **Impact of Perceived Security on Consumer Trust in Online Banking**, Auckland New Zealand, 2007, P 22.

[3] علوطي لمين، **تحديات الأمن الإلكترونية في المؤسسة، مجلة أبحاث اقتصادية وإدارية**، العدد 06، 2009، ص 167.

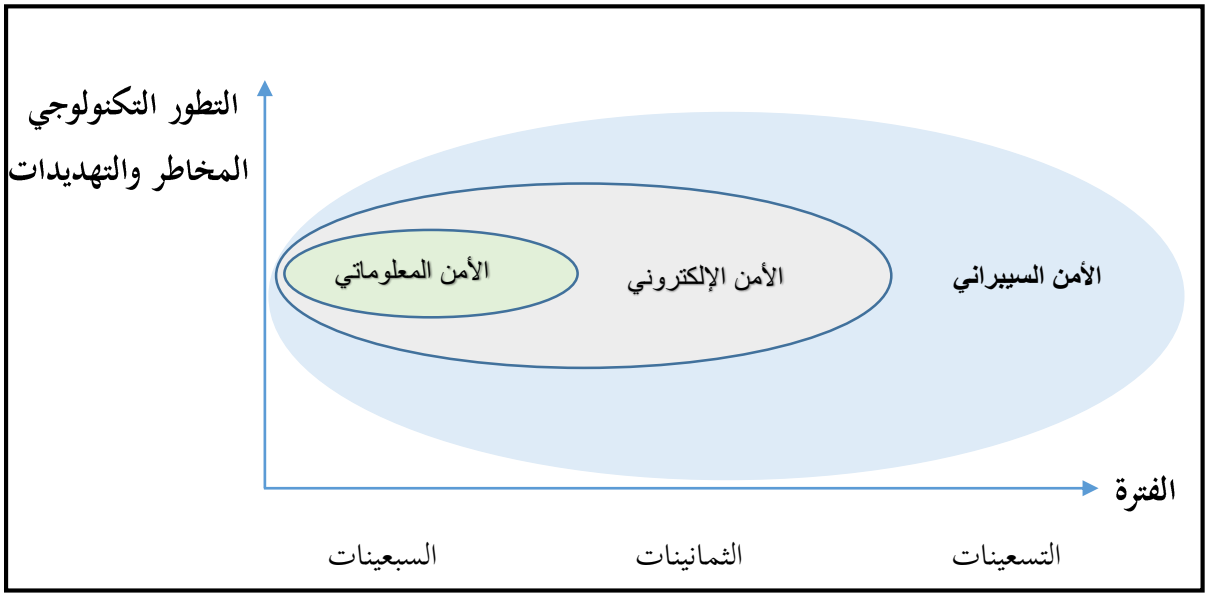
[4] نور الدين بربار، **دور الأمن المعلوماتي في تفعيل نشاط الصيرفة الإلكترونية**، مجلة الاقتصاد والتنمية، مخبر التنمية المحلية المستدامة، المدية، العدد 02، 2014، ص 21.

كذا مؤشرات مقياس (فريدة حمودي، 2020)[1]، (Qais Hammouri et al، 2021)[2].

المطلب الخامس: الفرق بين الأمن السيبراني والأمن المعلوماتي والأمن الإلكتروني

عند بدء البحث في موضوع الأمن السيبراني (Cyber Security) صادفتنا عدة مصطلحات مشابهة له، منها الأمن المعلوماتي (Information Security)، والأمن الإلكتروني (Electronic Security)، إلا أنه ومن خلال تعميق البحث، تبين لنا أن هذه المصطلحات هي تعبر عن مراحل زمنية متلاحقة ومتسلسلة مرَ بها الأمن السيبراني، ويوضح الشكل التالي التطور التاريخي لمفهوم للأمن السيبراني وفق زيادة مستوى التطور التكنولوجي وزيادة المخاطر والتهديدات السيبرانية عبر الزمن.

الشكل رقم (I-2): التطور التاريخي لمفهوم الأمن السيبراني



المصدر: من إعداد الطالب بالاعتماد على تاريخ الأمن السيبراني.

برز في بداية سنوات السبعينات الاهتمام بالمعلومة كمصدر للتفوق التنافسي أو الميزة التنافسية، فجاء تطبيق الأمن لحماية كل ما يتعلق بجمع وإيصال وتخزين ومعالجة المعلومات داخل المؤسسة من محاولات المنافسين للحصول عليها بطرق غير شرعية وغير مسموح بها، إلى جانب الحماية المادية والفيزيائية (الورقية)، حيث أطلق عليها مصطلح أمن المعلومات أو أمن نظم المعلومات في المفهوم التقليدي، ومع الانتشار الواسع لاستخدام

[1] فريدة حمودي، **الأمن المعلوماتي في الجزائر بين التطورات التكنولوجية وضعف البيئة الرقمية للمجال المصرفي**، مجلة جيل أبحاث قانونية معمقة، العدد 41، 2020، ص 91.

[2] Qais Amiri, Tahaer Majali, Damaithan Almajali, Abdalrazzaq Aloqool, Jassim Ahmad Al-Gasawneh, **Explore the Relationship between Security Mechanisms and Trust in E-Banking**: **A Systematic Review**", Annals of R.S.C.B, ISSN: 1583-6258, Vol 25, N 6, 2021, PP 17083-17093, Https://annalsofrscb.ro, Retrieved: 09-01-2022, 20:10.

تكنولوجيا المعلومات والاتصال (TIC)، اتسع مفهوم أمن المعلومات ليشمل حماية الأعمال الإلكترونية في المؤسسة والإدارة إشارة إلى مفهوم أشمل وأوسع منه يتضمن حماية التعاملات الإلكترونية بين أطراف الإدارة الداخلية للمؤسسة، وبينها وبين العالم الخارجي، ليصبح يُطلق عليه الأمن الإلكتروني وهذا في سنوات الثمانينات، أما بعد ذلك ظهر مفهوم الأمن السيبراني (Cyber Security) الذي يهتم بأمن كل ما هو موجود على السايبر أو ما يسمى بالفضاء السيبراني* وكان أول من تطرق لذلك الباحثان جون أركويل (John Arqyile) وديفيد رونفليد (Davied Ronfeld) في عام 1997م في كتابهما الموسوم بـ: "الحرب السيبرانية القادمة".[1]

عليه، وبناءً على ما يمثله الشكل رقم: (I-2) لم تُلغ المفاهيم السابقة (الأمن المعلوماتي والأمن الإلكتروني)، وإنما توسعت إلى مفهوم شامل (الأمن السيبراني) الذي يتكيف مع التطورات التكنولوجية والمخاطر والتهديدات السيبرانية والرهانات المختلفة على الصعيد الاستراتيجي كالحروب السيبرانية والدفاع الرقمي، وعلى الصعيد القانوني كالمراقبة الإلكترونية وحماية الحياة الخاصة، وعلى الصعيد الاقتصادي كالتنافسية والحاجة إلى الإبداع الرقمي.[2]

وبهذا فالأمن السيبراني له مفهوم أوسع من أمن المعلومات ومن الأمن الإلكتروني، فأمن المعلومات يهتم بأمن المعلومات المادية والفيزيائية (الورقية)، والأمن الإلكتروني يهتم بالدفاع عن البيئة المادية (جميع الأصول غير معلوماتية) التي تتألف من ترابط شبكة البنى التحتية للمعلومات التي تتضمن أنظمة شبكة الاتصالات السلكية واللاسلكية وأنظمة الحواسيب وأجهزة التحكم، وأنظمة التشغيل والألياف الضوئية والكابلات والاتصالات الفضائية عبر الأقمار الصناعية، بمعني هو ليس افتراضي، أما الأمن السيبراني فهو يهتم بأمن كل ما هو موجود على السايبر (الفضاء السيبراني) والذي من ضمنه أمن المعلومات والأمن الإلكتروني.

وهنا يعني أن الأمن المعلوماتي والأمن الإلكتروني والأمن المادي وغيرها من الأنظمة القادمة سوف تكون تحت مظلة الأمن السيبراني.[3]

المبحث الثاني: مفهوم البيانات الشخصية

في مجال الاقتصاد مصطلح البيانات جد مهم، فهي تمثل أصولًا تساهم في تحسين أداء وإنتاجية المؤسسات، كما تساعد في اتخاذ القرارات الاستراتيجية الهامة واستشراف المستقبل وتعزيز مقومات الميزة التنافسية، خاصة على المستوى المصرفي فهي ذات قيمة جد عالية باعتبارها موردا هاما يتعلق بخصوصية عملائها، إذ يتعين عليها ضمان حمايتها وحسن استغلالها بما يعزز ثقة أصحابها في المؤسسة الخدمية المصرفية.

(*): **الفضاء السيبراني**: يعني الفضاء الذي أوجدته تكنولوجيا المعلومات والاتصالات (TIC) في مقدمها الإنترنت، حيث يرتبط ارتباطا وثيقا بالعالم المادي عبر البنى التحتية للاتصالات كالحواسيب ونظم الكمبيوتر والأنظمة المعلوماتية والهواتف، ولا يقتصر على الإنترنت فقط، وانما أيضا على الشبكات العالمية مثل: swift-gsm-acars.

[1] محمد محمود العمري، **المرجع السابق نفسه**، ص 25.

[2] Refalo pierre, **La Sécurité Numérique de L'entreprise l'effet papion du hacker**, Eyrolles, Paris, 2013, P 27.

[3] **الموقع**: (https://www.rattibha.com)، تاريخ الاطلاع: 08-04-2022، الساعة 17:40.

المطلب الأول: تعريف البيانات الشخصية (Personal Data)

يُشير مفهوم البيانات إلى مجموعة حقائق غير مُنظمة فقد تكون في شكل أرقام أو حروف أو كلمات أو رموز أو صور لا علاقة بين بعضها البعض، فهي لا تؤثر في سلوك من يستقبلها كون ليس لها معنى حقيقي، فهي حقائق غير مرتبطة وغير محددة العدد، ومن الأمثلة عن البيانات: عدد المستخدمين، أسماء العملاء، الطاقة الإنتاجية، قيمة مرتبات العاملين، البريد الإلكتروني لهم...الخ، وبالتالي يتم تشغيل هاته البيانات بغرض تحويلها إلى معلومات مفيدة لاستغلالها في عملية اتخاذ القرار، فالبيانات بصورتها الخامة هي لا تعطي دلالة.

البيانات المطلوبة يتم جمعها إما من داخل المنظمة وتُسمى البيانات الداخلية على سبيل المثال الأرقام التي توضح حجم المخزون، الحصة السوقية، أرقام المبيعات، معدلات الإنتاجية، التكاليف المختلفة، كما تجمع البيانات أيضا من خارج المنظمة ويطلق عليها بالبيانات الخارجية، كالبيانات المتعلقة بالمنافسين، العملاء، الموردين، الجهات الحكومية التي تتعامل معها المنظمة، بالإضافة إلى وجود العديد من الوسائل التي تُستخدم في جمع البيانات كالمسح الاحصائي من خلال قوائم الاستقصاء، الملاحظة، المقابلات المتعمقة...إلخ.[1]

البيانات هي: "حقائق وعناصر أولية (Raw Facts)، أو مادة خام، وتعني معطيات لم تُعالج يدويا أو حاسوبيا لاستنباط معانيها واستجلاء سياقها العام أو محتواها أو مضمونها، وبذلك هي المادة الأساسية للمعلومات".[2]

أما بالنسبة للبيانات الشخصية: فهي: "البيانات العائدة إلى شخص معين، التي يمكن أن تساعد على تحديد هويته، والتعرف إليه، كالاسم الشخصي، والصور الشخصية، ورقم الهاتف، ومعلومات عن العمل والمسكن، والبريد الإلكتروني، والحساب البنكي، وغيرها".[3]

عرفها المشرع الجزائري ضمن المادة الثالثة من القانون: 07-18، المؤرخ في: 25 رمضان عام 1439هـ، الموافقـ: 10 يونيو 2018 م، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي بأنها: "كل معلومة بغض النظر عن دعامتها متعلقة بشخص معرَف أو قابل للتعرف عليه والمشار إليه أدناه، "الشخص المعني" بصفة مباشرة أو غير مباشرة، لاسيما بالرجوع إلى رقم التعريف أو عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الثقافية أو الاقتصادية أو الاجتماعية.[4]

ومن هنا فالبيانات الشخصية هي: المورد الأساسي في اتخاذ القرارات المالية، واستخداماتها لا حصر لها من حيث فهم سلوك التسويق للعملاء، وأنماط الانفاق، واستهداف الإعلانات، وتقديم توصيات المنتجات ذات

---

[1] نوري منير، **نظام المعلومات المطبق في التسيير**، ديوان المطبوعات الجامعية، طبقة 1، الجزائر، 2015، ص 48.

[2] سعد غالب ياسين، **نظم إدارة قواعد البيانات**، دار اليازوري العلمية للنشر والتوزيع، عمان، الأردن، 2010، ص 21.

[3] فؤاد أمين السيد محمد، **جرائم مراقبة المراسلات الإلكترونية، دراسة مقارنة**، دار النهضة العربية، القاهرة، مصر، الطبعة الأولى، 2016، ص 39.

[4] بيدري ربيعة، **دور الأمن السيبراني في حماية المعاملات المالية المصرفية المبرمة في الشكل الإلكتروني**، إصدارات المركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية، الجزء الأول، برلين، ألمانيا، 2022، ص 468.

الصلة، حيث يتم استخدم هاته البيانات من قبل عمالقة التجارة الإلكترونية مثل: علي بابا، أمازون، لاستهداف الزبائن من أجل البيع المضاعف وارسال ومتابعة العروض الشخصية.[1]

المطلب الثاني: العلاقة بين البيانات والمعلومات والفرق بينهما

العلاقة الوطيدة بين مصطلحي البيانات والمعلومات تجل من مستخدميها النظر إليهما كمترادفين رغم الفرق الشاسع بينهما وأن لكل منهما مدلوله الخاص، وهذا ما ستنطرق إليه.

❖ العلاقة بين البيانات والمعلومات:

إن علاقة البيانات بالمعلومات هي كعلاقة المواد الخام بالمنتج النهائي، بمعنى أن أنظمة المعلومات هي من تقوم بتشغيل البيانات وإعدادها وتحويلها من صورة لا تقبل الاستخدام إلى صورة يمكن فيها استخدام هاته البيانات فتُحول على شكل معلومات، كما ينبغي الإشارة إلى حقيقة أساسية أن ما يُعد حاليا معلومة بالنسبة لشخص معين، قد تكون بيان خام بالنسبة لشخص آخر، مثلا أسماء الطلبة الناجحين ليس له معنى، وإذا تم تصنيف هؤلاء الطلبة على أساس المعدلات التي تحصلوا عليها فهنا تم تحويل البيانات إلى معلومات أصبحت ذات قيمة لإدارة الجامعة، بل وبالنسبة لنفس الفرد فإن المعلومة يمكن أن تكون بيان خام في موقف آخر مختلف بسبب وجود العلاقة التزامنية بين البيانات والمعلومات.

من هنا يجب التفرقة بين مصطلحي (البيانات والمعلومات) لأن هناك من يستخدمهما كمترادفين رغم أن لكل منهما مدلوله الخاص، كما يمكننا القول أن المعلومات تُنتج أو تُشتق من البيانات والعكس غير صحيح، فالبيانات (Data) أو (Donnees) هي: مدخلات للحاسب الإلكتروني (In Puts)، إذ تُعتبر المادة الخام التي يتم تشغيلها في نظام المعلومات فتنتج مخرجات (Out Puts) وتُسمى المعلومات (Informations) الناتجة عن معالجة البيانات التي تم إدخالها، وهذا ما يؤكده التعريف اللغوي لكل من المعلومات والبيانات، فالقاموس يُعرَف البيانات أنها: "حقائق أو أشياء معروفة يقينًا، يمكن من خلالها الوصول إلى نتائج معينة، أما المعلومات فهي تقدير معرفة أو أخبار، بمعنى أي شيء يُضيف إلى الفرد معرفة جديدة، وبمعنى آخر هي: "المعنى الذي يُستخلص من البيانات".[2]

أما بالنسبة لعملية معالجة البيانات، فهي عبارة عن ترتيب هذه البيانات بطريقة معينة، فيؤدي ذلك بتحولها إلى حقائق ذات قيمة وبالتالي يمكن استخدامها، كما نشير أن عملية معالجة البيانات وتشغيلها يتطلب ضرورة توافر عناصر معينة كالمعدات والآلات المستخدمة في التشغيل، وأيضا أفراد لديهم معرفة يقومون بتلك العملية بالطرق والإجراءات الصحيحة المتبعة لتشغيل تلك البيانات.

---

[1] جهاد أحمد السيد محمد، **أهمية الشبكات في مؤسسات الدفع الإلكتروني**، إصدارات المركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية، الجزء الأول، برلين، ألمانيا، 2022، ص445.

[2] حمام عبد اللطيف، عبد الشافي حنفي معوض، **الحماية الجنائية للبرامج والبيانات المعالجة إلكترونيا، دراسة مقارنة**، رسالة قدمت لنيل درجة الدكتوراه حقوق، جامعة القاهرة، مصر، 2017، ص 20.

وبالرغم من هذا الفرق بين المعلومات والبيانات فإنه لا يمكن وضع حد فاصل بين ما يُعتبر بيانات (مدخلات) وما يُعتبر (مخرجات) كون التداخل قائم بينهما، فما يعد معلومات في مرحلة من المراحل يُعد بيانات في مراحل أخرى إذا أجري عليه أي معالجة.[1]

يمكن اختصار ما سبق ذكره، في الجدول التالي لتبيين الفرق بين البيانات والمعلومات وبنوع من التفصيل:

الجدول رقم (I–1): الفرق بين البيانات والمعلومات

الرقم	البيانات	المعلومات
1	حقائق في شكلها الخام هي غير مصنفة أو مفهومة، تم تجميعها بغية استخدامها للوصول إلى معلومات مفهومة.	حقائق تم تجهيزها فأصبحت مفهومة ومعدة للاستخدام.
2	حقائق تم الحصول عليها عن طريق الملاحظات أو عن طريق أجزاء بحوث تجريبية.	حقائق تم الحصول عليها عن طريق تشغيل مجموعة من البيانات الخام المرتبة والمجهزة.
3	حقائق تتضمن الكلمات والرموز والأرقام والأشكال التي تعبر عن مواقف أو أفعال إدارية معينة.	حقائق تمثل معاني مشتقة ومستخلصة من البيانات بهدف حدوث تغيُر في معرفة وإدراك الشخص أو من قام باستلام هذه البيانات.
4	هي مدخلات لنظام المعلومات.	هي مخرجات لنظام المعلومات.

المصدر: سليماني عادل، مطبوعة في مقياس تدقيق ومراقبة نظام المعلومات، تخصص تدقيق ومراقبة التسيير، قسم العلوم الاقتصادية، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة غرداية، 2018، ص 37.

المطلب الثالث: الرقابة على أمن بيانات العملاء في المصارف الإلكترونية

يتوقف اعتمادنا على البيانات التي تقدمها نظم التشغيل إلى حد كبير على مدى فعالية وكفاية إجراءات الرقابة على أمن النظام بشكل عام (الأجهزة والبيانات)، كون ضُعف إجراءات الرقابة يُسبب ويؤدي إلى التشغيل غير المصرح به لمختلف العمليات، وكذا انتهاك سريتها، وفقدان الأصول والبيانات الهامة، كما تهدف الرقابة على أمن البيانات إلى المحافظة على خصوصية البيانات وسلامتها داخل نظام الحاسب من الفقد أو الوصول غير المسموح به لهذه البيانات أو فسادها، وأهم إجراءات تنفيذها هي على النحو التالي:[2]

[1] أسامة عبد الله قايد، **الحماية الجنائية للحياة الخاصة وبنوك المعلومات دراسة مقارنة في القانون الفرنسي والأمريكي والمصري وفقا لآخر التعديلات التشريعية**، دار النهضة العربية، بدون رقم طبعة، القاهرة، 2015، ص 77

[2] سعد محمد أبو كميل، **تطوير أدوات الرقابة الداخلية لهدف حماية البيانات المعدة إلكترونيا، دراسة تطبيقية**، رسالة ماجستير، غزة، فلسطين، 2011، ص ص 69-72.

1-تقييد عملية الوصول للبيانات: يهدف ذلك إلى منع أي شخص غير مصرح له بالوصول للبيانات عن طريق الحواجز أو العوائق سواء كان من داخل المنشأة أو من خارجها.

2-العزل: ونقصد به عزل البيانات الحساسة عن طريق وضعها في مكان لا يسمح بالوصول غير المشروع لها، مثل: حفظ توثيق البرامج وملفات البيانات، مع منع الوصول إليها إلا الشخص المسؤول فقط.

3-التصريح بالاستخدام: نقصد به تخصيص شفرات (حروف أو أرقام، أو خليط منهما) للأشخاص المسموح لهم فقط لكي يستخدموها عند الحاجة للوصول إلى البيانات، كما يمكن أن يجري البرنامج حوارا أو اجراءً تقنيا معينا مع المستخدم للتعرف عليه قبل أن يسما له بالاستمرار في التشغيل.

4-تقييد الاستخدام: يكون من خلال السماح للشخص بالوصول إلى بيانات معينة فقط، ويمنع من الوصول إلى بيانات أخرى، كما قد يسمح له بالوصول إلى بيانات معينة في مواعيد العمل الرسمية فقط، أو كذلك يسمح له بإدخال البيانات فقط دون تشغيلها أو تحديثها، وعلى سبيل المثال يمكن ضبط الوحدة الطرفية (كالبطاقة الإلكترونية البنكية) فنجعلها تتوقف عن العمل بعد عدد معين (ثلاثة أو أربعة مرات) لمحاولات الوصول من شخص غير مصرح له ذلك.

5-التشفير: ويقد به عدم نقل البيانات الحساسة والهامة جدا في صورتها العادية بل يتم نقلها في صورة شفرات أو رموز لا يعرفها إلا مستخدمها المصرح له بذلك، وبحيث لو وقعت مع شخص غير مسموح له فلن يفهم منها شيئا، فهذا أسلوب يستخدم لضمان سرية وخصوصية وسلامة البيانات التي يتم تبادلها بين الأطراف المختلفة.

6-التدمير: ويقصد بالتدمير التخلص كليا وبصفة نهائية من البيانات الحساسة جدا حين الانتهاء من استخدامها، إما بمحوها إذا كانت على وحدات تخزين أو حرقها إذا كانت مطبوعة.

7-استعادة البيانات: قد يحدث فقدان أو ضياع البيانات لسبب أو لآخر مثلا: خطأ في التشغيل أو تلف في وحدات التخزين أو عطل مفاجئ في الأجهزة، ففي هذه الحالة يجب أن يكون هناك وسيلة لاستعادة هذه البيانات فورا، لذا الاحتفاظ بنسخة احتياطية من ملفات البيانات والبرامج، والوثائق وقواعد البيانات هو واجب، مع إلزامية الاحتفاظ بهذه النسخة الاحتياطية في مكان بعيد وآمن عن مكان نظام الحاسب، مع إمكانية تحديد المدة أو الفترة التي سيُحتفظ بهذه النسخة، ومن أشهر خطط استعادة البيانات بعد ضياعها أو فقدها هو إجراء يُطلق عليه (الجد-الأب-الابن)، حيث يتم تجميع ثلاثة أجيال من الملف الرئيسي ويتم الاحتفاظ بها على مدار الوقت، فإذا فقدنا ملف الأب والابن فإنه يمكن استخدام ملف الجد لأجل استعادة ملف الأب ثم يتم استخدام ملف الأب لأجل استعادة ملف الابن، فهذا المدخل أساسا يستخدم لاستعادة البيانات المخزنة على الشرائط الممغنطة، بالإضافة إلى أن تجديد أي ملف إلكترونيا يستوجب له ملفان الأول تُقرأ منه البيانات والثاني تُنقل إليه البيانات بعد تعديلها، وبهذا باستخدامنا لهذا المبدأ في أي مشروع نضمن أن يكون لنا احتياطي كافي من الملفات حتى نؤمن سلامتها ونحفظ البيانات المسجلة عليها.

ومما سبق، يمكن القول أنه يجب حماية البيانات والبرامج أيضا من الأخطاء المتعمدة وغير المتعمدة، ومن أي استخدام غير مصرح به، فقد تتصف البيانات المخزنة بسرية عالية وحساسية كبيرة ما يوجب حمايتها من أي سوء استخدام عن طريق اتباع أساليب وقائية تحميها، والجدير بالذكر أنه لا يوجد على الإطلاق نظام أمني يمنع حدوث تلك الأخطاء أو المخاطر والتهديدات، ولكن الهدف هو تقليل احتمالات حدوثها إلى أقل حد ممكن.

8-الرقابة المتخصصة من خلال التطبيقات: يعد هذا الإجراءات أسلوبا متخصصا لأجل رقابة تدفق البيانات خلال أداء وظائف نشاط معين، فهي تُصمم لضمان أمن وصول البيانات وكذا دقة إتمام العمليات المطلوبة، وتستهدف هذه الإجراءات منع حدوث أي خطأ وضبطه إذا حدث، وتصحيح الأخطاء المحتملة خلال مسار البيانات داخل نظم التطبيقات، والهدف العام لرقابة التطبيقات هو التحقق من أن العمليات المصرح بها تم تشغيلها والتقرير عنها بالدقة المطلوبة، كما يتم ممارسة هذه الرقابة في كل مراحل تدفق البيانات داخل هذا النظام، ويمكننا أن نقول أنَ أساليب الرقابة على التطبيقات هي أساليب رقابة وقائية أكثر من أنها رقابة بالتغذية العكسية، والعديد منها يضمن اكتشاف الأخطاء التي يصعُب اكتشافها، إذ يمثل ذلك عاملا هاما في ظل كثرة النظم الإلكترونية أين يفقد عنصر الفطنة والفراسة البشرية وقدرة الإنسان على التحكم.

9-تقييم عمل الرقابة: يجب أن تهتم إدارة المنظمة وتشارك في أعمال الرقابة، وكذا تتأكد من أن نظام الرقابة الموضوع هو حقا النظام المطبق، فعادة تُشكل لجنة لتقييم ذلك، هذه الأخيرة يجب أن تتمتع بالاستقلال التنظيمي عن كل المستويات والوظائف الأخرى لأجل مراجعة عمل الأنظمة والشبكات وجميع الأجهزة والخوادم والتطبيقات التقنية.

المطلب الرابع: آلية التخزين السحابي لبيانات العملاء في البنوك الإلكترونية

هناك خياران معتمدان لتخزين البيانات: وهما التخزين الداخلي والتخزين السحابي، فقد كان في الماضي تطوير تطبيقات البيانات يعتمد أساسا على حفظ هذه البيانات في وسائط تخزين داخلية (من خلال الخوادم داخل الشركات أو المؤسسات)، فتطلب ذلك توفر مستودعات بيانات عالية التكلفة، بالإضافة إلى تثبيت برامج جد معقدة لإدارة تلك المستودعات.

فالتطورات الحديثة في علوم الحوسبة والبيانات ساهمت كثيرا في استبدال تلك الطريقة من خلال التخزين السحابي، الذي يُعد بمثابة حل أمثل لتخزين البيانات حتى وإن كانت ضخمة، وذلك لما يلي:

أ-توافر نظام عالي السرعة على نطاق واسع يُسهل حركة البيانات من مكان إلى آخر، بالإضافة إلى وجود بيانات منتجة محليا لم يعد هناك حاجة لتخزينها داخليا، وأصبح بالإمكان نقلها وتخزينها سحابيا.

ب-أصبحت جل التطبيقات الإلكترونية تعتمد على التخزين السحابي، ما يعني أن عملية إنتاج مختلف البيانات وتخزينها سحابيا تزداد باستمرار، كما ساهم ذلك في قيام رواد الأعمال بعمل تحليلات متطورة للبيانات الضخمة

وهذا لمساعدة الشركات والمؤسسات في كثير من المجالات والأنشطة مثل معاملات التجارة الإلكترونية وبيانات الأداء عبر تطبيقات الويب.

هناك جوانب متعددة للتخزين السحابي جعلت منه خيارا أفضل للشركات والمؤسسات، فمثلا يمكن أن يشمل التخزين السحابي أنظمة النسخ الاحتياطي وكذلك أنظمة تخزين البيانات الضخمة.

وتوجد الكثير من خيارات مزودي هاته الخدمات، مثل شركات مايكروسفت وأمازون وقوقل للتخزين السحابي فهي توفر أمن وحماية البيانات والخصوصية، وكذا قابلية التوسع مع تكلفة معقولة لهذه الخدمات عن طريق النسخ الاحتياطي السحابي للبيانات، كما يمكن للمؤسسات الاستفادة من هذا النوع من الخدمات من خلال مراكز البيانات التي تمتد عبر مواقع جغرافية متعددة، وهذا يضمن لها التوافر الدائم للبيانات واستعادتها في حال فقدانها بسهولة، كما يمكن نسخ البيانات احتياطيا عبر عدة مراكز بيانات مختلفة في مناطق متوزعة عبر العالم باستخدام التخزين السحابي، بهدف عدم الاحتفاظ بالنسخ الاحتياطية في مكان واحد فقط.

تقنيات التخزين السحابي هي توفر خصائص أخرى للحماية للنسخ الاحتياطية، فمقدمو تلك التقنيات هم يضمنون حماية البيانات المنسوخة احتياطيا عبر تقنيات التشفير المتقدمة والحديثة وهذا قبل القيام بنقل البيانات وخلال نقلها وكذلك بعد نقلها.[1]

أيضا معالجة البيانات هي تتطلب سعة تخزين وقوة معالجة، فأما من حيث السعة التخزينية التقنيات السحابية تفي بهذا الأمر، حيث يمكن للشركات والمؤسسات الحصول على خدمات التخزين القابلة للتوسع بيُسر، ويمكن كذلك لهذه التقنيات تلبية متطلبات الحوسبة لأجل تحليل البيانات الضخمة، فخبراء تحليل البيانات هم يُوصون باستخدام الخدمات المدعومة سحابيا بهدف القيام بعمليات تحليل إدراكهم بالإمكانيات التي توفرها هاته التقنيات.

ومن أهم مزايا تخزين البيانات سحابيا نجد ما يلي:

-يوفر التخزين السحابي بُنية تحتية هي متاحة بسهولة، مع قدرته على التوسع والتعامل مع أي مقدار من البيانات ومتطلبات التخزين.

-يؤدي تخزين البيانات سحابيا إلى التخلص أو تقليص الاحتفاظ بالأجهزة والبرامج والموظفين، ويُعد نموذج الحوسبة السحابية المبني على الدفع حسب الحاجة إلى الخدمات هو الأكثر فعالية من حيث التكلفة، وهذا ما يساهم في خفض التكاليف وزيادة الكفاءة والحد من هدر مختلف الموارد.

-الحوسبة السحابية ترفع من كفاءة استخدام الموارد الإلكترونية، فهي توفر الوقت المبذول لأجل الحصول على البرامج أو الخدمات الإلكترونية، وكذا توفر إمكانية الوصول إلى الخدمات بكل سهولة وبسعة أكبر.

[1] وزارة التعليم للملكة العربية السعودية، **علم البيانات**، مسار الثانية ثانوي، الناشر شركة تطوير للخدمات التعليمية، 2022، ص 24، على موقع: www.arabia2.com/vb، تاريخ الاطلاع: 08-07-2023، الساعة: 10:00.

-توفر المزيد من المرونة خاصة في مطابقة موارد تكنولوجيا المعلومات والوظائف العملية التي تعتمد الأساليب التقليدية للحوسبة، وتوفر أيضا زيادة حركة العملاء بتمكينهم الوصول إلى معلومات الأعمال وكذا التطبيقات بتوفير مجموعة واسعة من الخدمات والمواقع، كما أن خدمات الحوسبة هي توفر سهولة ومرونة أكبر في أداء المهام المختلفة، وتُتيح إمكانيات الربط بين مواقع إلكترونية عديدة، مثل الشبكات الاجتماعية.

- تطبيقات الحوسبة السحابية تجعل المؤسسات تستغني عن اعتماد شراء الأجهزة، وخدمات التركيب، والتشغيل والصيانة، وتراخيص البرامج، وغير ذلك.[1]

-تركز المؤسسات والشركات على عمليات تحليل البيانات بدلا توزيع جهودها على إدارة البنية التحتية، وهذا ينعكس بشكل إيجابي على فعالية الأداء والميزة التنافسية.

- إمكانية استخدام الحواسيب للوصول إلى الموقع من أي مكان، مما يزيد من أمان البيانات وجعل الأداء أفضل مما كان عليه.

-تكنولوجيا التخزين السحابي هي صديقة للبيئة كونها تعمل على تقليل عدد الأجهزة المستخدمة والماكينات وتوفر الطاقة، وبالتالي ينعكس ذلك على التكنولوجيا الخضراء.[2]

المطلب الخامس: أنواع التهديدات السيبرانية الماسة بأمن بيانات العملاء (Types of Cyber Threats to Customer Data Security)

إن الاعتداء على أنظمة الدفع الإلكترونية هي من بين سلبيات التطورات التكنولوجية، فهي لم تسلم من المخاطر والتهديدات أو الجرائم السيبرانية، أو بما يصطلح عليها كذلك بجرائم الحاسوب والإنترنت، جرائم التقنية، جرائم الجيل الخامس، الجرائم الإلكترونية، فهي مصطلحات مختلفة لمفهوم واحد يُفيد الجريمة السيبرانية على وجه العموم، على سبيل المثال في البنوك تتم من خلال البطاقات الإلكترونية البنكية يفَك شفرتها، أو الاستعمال غير المشروع لها من خلال الاعتداء على البيانات والأرقام، فيتم قرصنتها من خلال أرقامها السرية، سواء بطريقة غير عمدية كالثغرات الأمنية في النظم والبرامج والشبكات وأخطاء المستخدمين، أو عمدية كهجوم الفيروسات، والتصيُد والتجسس والملاحقة الحاسوبية، وأسلوب الخداع الذي يتم بإنشاء مواقع وهمية، وأسلوب الاستدراج، وأسلوب تفجير المواقع الذي يمس في الغالب المؤسسات البنكية، وأسلوب اختراق البطاقات البنكية وكسر شفرتها لاستخدامها بأهداف إجرامية، كل هذا أدى إلى ظهور جرائم أخرى تدخل في إطار الإرهاب الإلكتروني، ومن بين أشهر مظاهر التهديدات السيبرانية الماسة بأمن بيانات العملاء، نجد ما يلي:

---

[1] إياد عماد علي، **الحوسبة السحابية**، دائرة تقنية المعلومات والاتصالات، البنك المركزي العراقي، 2023، ص 12، على الموقع: https://cbi.iq/static/uploads/up/file-152377270192790، تاريخ الاطلاع: 10-08-2023، الساعة: 14:50.

[2] عزة علي آل كباس، **التخزين السحابي**، 2017، ص 6، على الموقع: https://cutt.us/U3gSP، تاريخ الاطلاع: 10-08-2023، الساعة: 11:30.

1-الثغرات الأمنية: هي تحدث عادة بسبب وجود خلل في البرامج أو العتاد، فعندما يعرف المهاجم أو المجرم الثغرات تكون الفرصة سانحة له للقيام بعملية الهجوم، هنا يستخدم المهاجم البرمجية وتسمى (Exploit)، يعني برنامج مكتوب بغرض الاستفادة من مختلف الثغرات الأمنية، واستخدام هاته البرمجية يسمى في الأمن السيبراني بعملية الهجوم (Attack).

2-الثغرات البرمجية: تحدث الثغرات الأمنية في البرامج بسبب وجود خطأ في برمجة نظام التشغيل أو هفوة في برمجة أي تطبيق، وعلى الرغم من جهود المطورين في محاولة سد الثغرات إلا أنه دائما ما تظهر ثغرات جديدة، ويبقى يحتاج بعدها التطبيق لتعديل أو ترقية، والشركات الكبرى غالبا ما تقوم بتطوير نظام التشغيل من خلال إصدار تحديثات وترقيات خاصة بها، على سبيل المثال والأكثر شهرة حاليا يقوم مطورو البرامج الخاصة بالهواتف الذكية بتطوير وترقيات برامجهم بصفة دورية.

ففي عام 2015 حدث لشركة سيسكو (IOS) اختراق نظام تشغيلها الخاص والمثبت على الموجهات الخاصة بالشركة، حيث يسمى هذا الاختراق (Synful Knock)، فقد تمكن المهاجم من مراقبة جميع الاتصالات الداخلية للشبكة وأنشطتها، ليتمكن من إصابة معظم الأجهزة الموصولة بالشبكة، وقبل هذا الاختراق قام المجرم بتحميل نسخة غير كاملة من نظام تشغيل الشركة (IOS) على الموجهات.

ولتجنب مختلف الاختراقات يجب على المؤسسات والشركات التأكد من سلامة نظام التشغيل مع تحديثه بصفة دورية والتأكد من إجراء الصلاحيات الممنوحة والمحددة الأشخاص ذوي الاختصاص من أجل الوصول إلى العتاد، فالهدف من تحديث البرامج هو إبقاء مناعة قوية من وجود الثغرات الأمنية، ولأجل ذلك فبعض الشركات هي تُسخر فريق خاص للبحث عن الثغرات الأمنية مع انزال تحديثات لها قبل أن يكتشفها المخترقون، مع العلم أنه يوجد فرق خارج الشركة على سبيل المثال ذوي القبعات البيضاء، مهامهم البحث والتقصي عن الثغرات الأمنية الموجودة في النظام الأمني للشركات حيث يمكن تأجيرهم لفحص ذلك، ومن الأمثلة الأخرى على فرق تقصي الثغرات الأمنية المشروع الخاص بشركة جوجل المسمى زيرو "Zero".[1]

3-فيض الصوان: الصوان (Buffer) يقصد به الذاكرة المؤقتة التي تحمل البيانات الخاصة بالبرامج أثناء التشغيل، لكن عندما يقوم البرنامج بملىء هذا الصوان بالبيانات وتزيد كمية هذه البيانات عن حجمه فتفيض منه، ليتم كتابتها في عناوين لذاكرة غير موجودة أصلا، فتحدث مشكلة في البرنامج، عليه تنتج عن هذا ثغرة أمنية تستغل من قبل المهاجمين لتخريب أو تعطيل البرنامج.

4-المدخلات غير صحيحة: في بعض الاحيان لا يتم مصادقة المدخلات بشكل سليم (نقصد بالمصادقة التأكد من نوعية البيانات التي تم إدخالها) فينتج عن ذلك مشاكل في البرنامج، على سبيل المثال يتم إدخال صورة بأبعاد معينة في برنامج خاص بمعالجة الصور، هنا لو استطاع المهاجم أن يتلاعب بهاته الصورة كي تبدو

[1] الموقع: https://code.google.com/p/google-security-research/issues/list، تاريخ الاطلاع: 10-08-2023، الساعة: 22:30.

للبرنامج بتلك الأبعاد، يصبح من الممكن أن يقوم هذا البرنامج بحجز ذاكرة بأبعاد مختلفة فيقع في فخ أخطاء قاتلة (Fatal Error).

5-حالة التسابق (Race Condition): في هاته الحالة تتصارع البرمجيات على بعض الخدمات المشتركة، حيث يحدث ذلك عند استخدام في آن واحد أكثر من عملية مصدر معين، على سبيل المثال استخدام نفس مساحة الذاكرة في نفس الوقت، فهذه المشكلة تحدث بعملية تزامن الأحداث أو حين ترتيبها.

6-ضعف في أدوات النظام الأمني: حفظ البيانات الحساسة يتم بتقنيات مثل التشفير (Encryption)، والتفويض (Authorization)، والمصادقة (Authentication)، حيث يجب على مُطوري النظم الأمنية أن يقوموا باستخدام برمجيات موجودة من قبل وتكون مختبرة ومعتمدة من حيث قوتها، مع تجنب ببناء برمجيات من الصفر لأن ذلك يؤدي إلى احتمال وجود ضعف وثغرات أمنية بصفة أكبر.

7-أخطاء نظام التحكم في الوصول (Access Control): التحكم في الوصول هو عبارة عن نظام للتحكم بمن يصل، مثلا التحكم في الوصول الفيزيائي للعتاد، التحكم في الوصول للموارد كالملفات، حيث يكون التحكم في صلاحياتهم تجاه هذه الملفات من قراءة فقط أو قراءة وكتابة، فغالبا ما تحدث اختراقات بسبب وجود خلل في نظام التحكم في الوصول، لذا يجب أن نضع في الاعتبار أنه يمكن تجاوز كل برنامج الحماية الأمنية في حالة وصول المهاجم فيزيائيًا إلى الموارد، وبالرغم من حماية نظام التشغيل من الدخول غير المصرح به، إلا أنه يمكن الوصول إلى البيانات من خلال القرص الصلب بطريقة مباشرة، ولتجنب هاته المواقف يجب أن يتم استخدام تشفير البيانات عند حفظها وكذا تقييد الوصول الفيزيائي للعتاد ومراقبة الوصول الفيزيائي باستعمال الكاميرات.

8-ثغرات العتاد (Gear Gaps): عادة ما تحدث الثغرات الأمنية للعتاد بسبب وجود عيب في التصميم، مثلا يتم تصميم الذاكرة العشوائية باستخدام مكثفات متجاورة، ومن خلال هذا التجاور ممكن أن تتأثر إحداها بالأخرى، وبناء على هذا العيب في التصميم يقوم المهاجم باستغلال هذا التجاور للوصول إلى مناطق في الذاكرة بطريقة غير مصرح بها، وهذا يسمى بهجمة (Rowhammer)، إذا الثغرات الأمنية في موارد العتاد هي خاصة بجهاز معين ولا يمكن استغلالها في محاولة الوصول العشوائية، ومع أن هجمات العتاد هي هدف للهجمات الكبرى، إلا أن الحماية منها تتم بتوفير برمجيات ونظم أمنية فيزيائية بسيطة.

9-البرمجيات الخبيثة (Malicious Software): نقصد بها "أي برمجية تُستخدم لأغراض غير شريفة، على سبيل المثال إلحاق الضرر، سرقة البيانات، الوصول غير المصرح به، تخطي الحواجز الأمنية"، فهي تُسمى خبيثة نظرا لصعوبة إزالتها بعد التثبيت، وأبرز صورها: هجوم الحرمان من الخدمة (التعطيل) الذي عادة ما يستهدف

الشركات الكبرى والمؤسسات الحكومية، والمصارف المالية بهدف منع المستخدمين من الوصول إلى النظام،[1] وفيما يلي برمجيات خبيثة أخرى سنتطرق إليها بإيجاز:

أ. برامج التجسس (Spyware): هي برمجيات خبيثة تم تصميمها للتجسس وتتبع المستخدمين، فهي تسجل نقرات المفاتيح وتقوم بنسخ البيانات على الجهاز الضحية، كما تقوم بتفتيش ملفات تعاريف الارتباط "الكوكيز" لاستخرج منها المعلومات السرية مثل كلمات السر وأرقام بطاقات الائتمان وغير ذلك، حيث تحاول الدخول للنظام من خلال اختراق الحواجز الأمنية كأن تقوم بإدماج نفسها مثلا في البرنامج الخبيث حصان طروادة، بهدف التجسس وسرقة البيانات، على سبيل المثال فقد تم سرقة المعلومات الشخصية لأكثر من 106 مليون عميل في مصارف الولايات المتحدة الأمريكية وحوالي 140 ألف رقم تأمين اجتماعي لعام 2019، وكذا اختراق 260 مليون سجل في القطاع المالي في نفس الفترة، وقدرت الخسائر بحوالي 38 مليار دولار للشركات المالية الأمريكية وحدها.[2]

ب. برمجيات الدعاية والاعلان (Adware): هي برمجيات خُبيثة صممت خصيصا لإظهار إعلانات للمستخدمين دون رغبتهم في ذلك، فتثبيتها يتم من خلال تثبيت برامج غير موثوقة من الإنترنت، حيث أن بعضها يتخصص في إظهار الإعلانات فقط، والكثير منها يهدف إلى عملية التجسس.

ت. البوت (Bot): هو اختصار لكلمة روبوت، فهو برنامج خبيث يتم تحميله على جهاز الضحية بهدف تأدية وظيفة خبيثة بشكل تلقائي، حيث يتم الاستفادة القصوى من البوت من خلال استخدام شبكة الروبوت Botnet، أين يتم تسخير عدد كبير من الأجهزة حول العالم تتلقى الأوامر تلقائيا من الشخص المهاجم أو الجهاز المتحكم.

ث. برمجيات الفدية (Ransomware): وهي برمجيات خبيثة صُممت خصيصا للاحتفاظ بالبيانات الهامة المسروقة بهدف دفع الفدية، فهذه البرمجيات هي تصل إلى الجهاز الضحية وتقوم بتشفير البيانات الهامة داخله بمفتاح معين، ولا يُعطى هذا المفتاح للضحية إلا إذا دفع الفدية، فأحيانا يقوم بعض مهاجمي برمجيات الفدية باختراق الحواجز الأمنية بغية تعطيل النظام، هذا الأخير ينتشر عن طريق ملف تم تنزيله من شبكة الإنترنت ويقوم بالدخول للنظام من خلال ثغرات برمجية.

تتنوع أسباب قيام الهاكر بعمليات التطفل والاختراق للمواقع والتطبيقات والمنصات، منها ما هو سياسي كالاطلاع على قرارات حساسة أو لإحداث نوع من الفزع في قطاع معين، كما يحدث أيضا في مهاجمة عمليات مزودات أسماء النطاقات والتي من نتائجها تعطل وتوقف عدد من المواقع على الإنترنت، ومنها ما هو عسكري، وهناك أسباب أخرى مالية بحتة كالابتزاز المباشر أو ما يعرف ببرامج الفدية "Ransomware" من المتوقع

[1] مروة فتحي السيد البغدادي، **المرجع السابق**، ص 1476.

[2] **الموقع**: https://www.bbc.com/Arabic/world-49166226، تاريخ الاطلاع: 10-01-2024، الساعة: 22:00.

أن تصل هذه الأخيرة إلى نحو ثلاثة ملايين هجمة خلال السنوات المقبلة، وأن تصل أيضا مبالغ الفدية التي ستُدفع إلى حوالي 20 مليار دولار، مقارنة بـ 11،5 مليار دولار في أواخر سنة 2019، حسب مجلة "**سايبر كرايم**".

مع العلم أنه بلغت كمية الأموال التي تم تحويلها فعلاً إلى مجرمي برامج الفدية وقام الضحايا بالإفصاح عنها سنة 2020 نحو 370 مليون دولار وهذا يقدر بـ: 3،3 أضعاف ما كانت عليه سنة 2019 حسب شركة Chainalysis المتخصصة بتحليل سلاسل الكتل الخاصة بالعملات المشفرة، حيث أن هذه فقط الأرقام هي الرسمية المعلنة فقط ولا تشمل الطرق الأخرى للدفع خارج العملات المشفرة، وكذا ولا تشمل المدفوعات المختلفة التي تتم بسرية حفاظا على سمعة الفرد أو الجهة، وحسب شركة الاستجابة للاختراقات المسماة Covewere أنه بلغ متوسط الفدية المدفوعة في الربع الأول من سنة 2021 حوالي: 212 ألف دولار وهي الأعلى بنسبة ثلاثة واربعون في المائة 43% عن الربع السابق".[1]

ج. **برمجيات الذعر (Scareware)**: هذا النوع من البرمجيات الخبيثة يقوم بإقناع المستخدم على أنه يجب أن يقوم برَد الفعل وإلا ستحدث مشكلة، على سبيل المثال: ظهور في جهاز الحاسب رسالة تقول أنه "يجب عليك إنزال هذا البرنامج كي نزيل البرمجية الخبيثة في جهازك"، وعليه فخوف الضحية من هاته البرمجية الخبيثة يدفعه ويجعله يقوم بتحميل البرنامج، وبالرغم من أن جهازه سليم لا يحتاج إلى مثل هذه البرامج، ومعظم هذه البرامج تكون بهدف التخريب أو التجسس.

ح. **برمجيات الجذور الخفية (Rootkit)**: هذا النوع يُصمم لأجل اختراق أنظمة التشغيل مع تثبيت برنامج يسمى "خلف الباب"، حيث يستخدم المهاجم فيما هذا البرنامج للوصول عن بعد إلى الجهاز الضحية، فبرمجيات الجذور الخفية تقوم بالتسلل عن طريق الثغرات البرمجية لأجل الحصول على صلاحيات منها تعديل ملفات النظام، في أغلب الأحيان تقوم برمجيات الجذور الخفية بتعطيل أو تجاوز برامج المراقبة لاكتشاف الدخلاء، وهذا ما يُصعَب من اكتشاف هذه البرمجيات الخبيثة، وفي العادة يتم من جديد إعادة تهيئة الجهاز الضحية المصاب ببرمجيات الجذور الخفية مع تحميل نظام تشغيل جديد.

خ. **الفيروس (Virus)**: هو برنامج خبيث يقوم بالتطفل على البرامج الأخرى حيث يَنفذ معها ويتكاثر وينتشر، فهو متطفل يحتاج إلى وسيط للانتشار، حيث غالبا ما يكمن الفيروس إلى غاية قيام العميل بحدث ما، مثل فتح ملف مصاب أو ينشط حتى بدون تدخل العميل مثل الانتظار وقت أو تاريخ معين للقيام بالتنفيذ، فالفيروسات ممكن أن تكون خفيفة الضرر مثل عرض رسالة أو صورة، وممكن أن تكون شديدة وقوية الضرر كأن تقوم بإزالة ملفات معينة أو التعديل عليها، فالفيروسات هي أيضا تتحور أي تُغير من شكلها كي لا يتم اكتشافها من قبل

[1] فهد الحويماني، "**الاستثمار في شركات الأمن السيبراني**"، جريدة العرب الاقتصادية الدولية بالسعودية"، 21-09-2021.

البرامج الخاصة بمكافحة للفيروسات، العدوى تتم عن طريق ذاكرة (USB) أو الأسطوانات الليزرية أو حتى مشاركة الملفات على الشبكة والبريد الإلكتروني، هنا أمثلة كثيرة عن الفيروسات، أشهرها "فيروس شمعون" الذي ظهر في المملكة العربية السعودية شهر جانفي2017، كما ظهر قبل ذلك سنة 2012، عندما قام بهجوم على شركة رأس غاز القطرية، فيروس شمعون قام بتعطيل المواقع الإلكترونية الخاصة بالجهات الحكومية: كوزارة العمل، ووزارة التنمية الاجتماعية، بمعنى آخر قام باستهداف الحكومة بشكل أساسي، وفي الجهة المقابلة قام بمهاجمة شركة أرامكو وشركات أخرى للبترول في الخليج، حيث ينتشر الفيروس عبر الروابط الإلكترونية في البريد المشبوه، وكذا عبر ذاكرة الفلاش، فعندما يصل إلى شبكة الشركة أو المؤسسة الحكومية يقوم بالبحث عن كل المتصلين بها فيُصيبهم أيضا، كما أن الفيروس يستهدف تعطيل جهاز الحاسب من خلال مسح محتوياته عن طريق استبدال MBR سجل الإقلاع الرئيسي (Master Boot Record) بملفات أخرى من شأنها أن تشل الجهاز تماما.

د. حصان طروادة (Trojan Horse): هي برمجيات مختلفة تحمل في طياتها برامج خبيثة حيث تبدو كبرامج صديقة عند اختراقها للحواجز الأمنية، حيث تقوم باستغلال صلاحيات المستخدم حين يقوم بتشغيلها، وهي في أغلب الأحيان تلتصق بالصور وملفات الألعاب وملفات الفيديو والصوت، فحصان طروادة يختلف عن الفيروس في أن هذا الأخير يُلصق نفسه ببرامج تنفيذية ويقوم بالنفاذ معها، أما حصان طروادة فيقوم بالالتصاق مع الملفات ويعتبرها وسيلة لنقله من مكان إلى مكان آخر، فحصان طروادة يُضلَل المستخدم لقصده الحقيقي، فيبدون أنه تطبيق عادي لكن عند تنفيذه أو فتحه، يقوم بتشغيل بعض التعليمات البرمجية الخبيثة الضارة في الخلفية.[1]

ذ. الديدان (Worms): هي أيضا برامج خبيثة تقوم بتكثير نفسها أشكال مستقلة وتنتشر بسرعة عن طريق الثغرات الأمنية في الشبكة، فالديدان تقوم بإبطاء عمل الشبكة على عكس الفيروسات التي تحتاج إلى عائل، فالديدان هي تنتشر بشكل مستقل، حيث في البداية تحتاج إلى رد فعل المستخدم من خلال فتح ملف أو تحميل وإنزال برنامج لتقوم بعد ذلك بالانتشار بذاتها، الديدان والفيروسات تشترك في صفات كثيرة، حيث لها هدف واحد وتعرف ثغرات معينة تقوم بالاختراق من خلالها وتعرف أيضا كيف تنتشر وماذا ستفعل، على سبيل المثال قامت سنة 2001 بأكبر الاختراقات على الإنترنت ديدان تسمى الشفرة الحمراء "Code Red"، حيث أصابت حوالي 658 خادم حول العالم، وخلال تسعة عشر ساعة فقط انتشرت فأصابت أكثر من: 300.000 ثلاثمائة ألف خادم.

[1] شيري وليم سلامة، أنسيمون كمال عزيز، أحمد مصطفى الشيخ، **الأمن السيبراني للخدمات المالية والمصرفية**، إصدارات المركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية، الجزء الأول، برلين، ألمانيا، 2022، ص 361.

10- هجمات الرجل كوسيط (Man in the Middle Attack): من خلال هذه الهجمات يستطيع المهاجم أن يُسيطر على جهاز الحاسب وهذا دون علم صاحبه بذلك، ويكون هذا من خلال استخدام الرسائل المزيّفة عبر وسائل الاتصال المختلفة، ويسمى هذا بالاستدراج الإلكتروني، حيث تعد الأخيرة من أكثر حالات الانتشار بواسطة الهواتف النقالة أو الرسائل النصية الإلكترونية، كما تُعتبر المصارف والشركات التي تقدم خدمات استشارية إلكترونية مواقع جذابة لاستهداف عمليات الاستدراج،[1] حيث يقوم المهاجم بالاستيلاء على مختلف المراسلات التي يرسلها الضحية عبر جهازه مثلا: كأن يرسل بيانات بطاقة الائتمان الخاصة به لموقع أمازون للشراء، فيأخذ المتطفل تلك البيانات ويراسل المواقع الأخرى الخاصة بالضحية مثل حسابه البنكي، مواقع الشراء المختلفة وبهذا يسحب من رصيد البطاقة الائتمانية للضحية.

11- الهندسة الاجتماعية: يقصد بها الطرق ومختلف الوسائل الاجتماعية التي من خلالها يتم الوصول إلى الشخص وإقناعه بالإدلاء بمعلومات سرية أو تنفيذ فعل ما، تعتمد الهندسة الاجتماعية على أن الناس بطبيعتهم ودودين ومساعدين، من هنا يتم استغلال نقاط ضعفهم وقلة خبرتهم، مثلا تتلقى من شخص اتصالا هاتفيا يتظاهر لك أنه موظف بالبنك وأن هناك خلل أو ضرورة ملحة للدخول إلى حسابك من أجل إجراء بعض الإصلاحات، فتثق به وترسل له بياناتك الشخصية، أو مثلا استثارة الغرور لدى الشخص من خلال تفخيمه وتعظيم شأنه وذكره بما يحب حتى يعطي الثقة، كما يمكن الدخول من باب الطع لدى الأشخاص في المال.

12- هجمات قطع الخدمة (DoS) (Denial Of Service attack): هي نوع من أنواع الهجمات الشبكية التي ينتُج عنها تعطيل أو توقف خدمات الشبكة، كالتوصيل بالأجهزة وتشغيل البرامج الشبكية، ويوجد نوعين من هجمات قطع الخدمة هما:[2]

أ. **الإغراق بالطلبات**: في هذا النوع من الهجوم الخبيث يتم إغراق الخادم بالطلبات المسموحة وبكثرة بهدف شغل الخادم وتعطيله نهائيا عن التجاوب مع المستخدمين، ونتيجة لعملية الإغراق بالطلبات تتوقف الشبكة عن العمل بسبب زيادة الزحام المروري للبيانات وبذلك تتوقف الخدمات ويتعطل التواصل مع الأجهزة والتطبيقات الشبكية.

ب. **الحزم المعدلة**: يتم فيها تعديل الحزم بغرض توقيع الضرر قبل إرسالها إلى الجهاز الضحية فلا يستطيع بذلك التجاوب مع تلك الحزم، على سبيل المثال يقوم المهاجم بتمرير مجموعة حزم بها عدد معين من الأخطاء التي لا يمكن اكتشافها في التطبيقات، هنا يُحاول التطبيق اكتشاف الخطأ مما يأخذ ذلك وقتٌ طويل لمعالجة الكمية الكبيرة من الحزم، عليه يبطئ استجابته للمستخدمين الأبرياء، وفي مثال آخر يقوم

---

[1] صندوق النقد العربي، **سلامة وأمن المعلومات المصرفية الإلكترونية، اللجنة العربية للرقابة المصرفية**، أمانة مجلس محافظي المصارف المركزية ومؤسسات النقد العربية، العدد 76، أبوظبي، الإمارات العربية المتحدة، 2017، ص 8.

[2] أسامة حسام الدين، **نفس المرجع السابق**، ص ص 20-27.

المهاجم بتمرير كمية حزم وهمية فيقوم المستقبل بمحاولة معالجتها لكن يتعطل الجهاز نظرا لأنه لم يستطيع التعامل معها.

من هنا نستنتج أن هجمات قطع الخدمة تُحدث ضررا كبيرا في نظام الاتصالات للمؤسسة وتُخسرها المال والوقت في محاولة للتعافي من تلك الهجمات، فهي سهلة التنفيذ حتى من قبل أشخاص قليلو الخبرة.

13- الهجمات الخليطة (Blended Attack): هي عبارة عن هجمات منظمة تستخدم أكثر من تقنية لتحقيق هدف معين، كون المهاجم لديه خليط من الفيروسات، الديدان، برمجيات التجسس، أحصنة طروادة، مسجل نقرات المفاتيح، هجمات الخداع، البريد المزعج، وهدفه الأساسي من الهجمات الخليطة هو تركيب هيكل برمجي ضخم حيث يتكون من عدة برمجيات صغيرة، فيهدد بذلك وبشكل قطعي البيانات الخاصة بالمستخدمين ويُحدث عظيم الضرر لها.

مع وجود وعي لدى معظم المؤسسات والشركات بالمشاكل الأمنية المختلفة ووضع مجهود كبير لمنعها، فإنه لا توجد تدابير أمنية محددة تحل المشاكل بنسبة مئة في المئة 100%، مع العلم أن محاولات الاختراق هي دائمة الوجود وخصوصا لو كانت الجائزة كبيرة، لذلك يجب الوقاية وأخذ الحيطة والحذر قبل التعرض للاختراق، وإن تقدر ذلك بعد الاختراق يجب أن تتوفر تدابير أمنية للحد من الضرر الناجم عنها.

كما يجب أن نعلم أن الاختراقات الأمنية هي لا تؤثر فقط على النواحي التقنية كسرقة بيانات العملاء أو سرقة حقوق الملكية الفكرية أو تدمير قواعد البيانات، ولكنها أيضا تُؤثر على سمعة الشركة أو المؤسسة.

14- شبكة الروبوت: شبكة الروبوتات هي مجموعات من البوت، متصلة بالإنترنت ويتحكم بها مهاجم أو مجموعة قراصنة، حيث تتم العدوى للبوت عن طريق زيارة موقع إلكتروني، فتح ملفات بها عدوى، فتح مرفقات بريد إلكتروني، ويمكن أن تحتوي شبكة الروبوتات على الآلاف أو حتى مئات الآلاف من البوت، يمكن تفعيلها لأجل توزيع برمجيات خبيثة، أو توزيع بريد إلكتروني مُزعج، أو تنفيذ بحث غاشم من كلمات السر، أو عمل هجوم مُوزع لتعطيل الخدمة DDoS، حيث يتم التحكم في شبكة الروبوت عن طريق خادم ويتم التحكم في هذا الأخير بالأوامر ويسمى بالخادم المتحكم، لتمكين مجرمو الأمن السيبراني بتأجير شبكات الروبوت مقابل الحصول على المال لطرف ثالث بالهجمات الخبيثة.

المبحث الثالث: إستراتيجية الأمن السيبراني ووسائل حماية البيانات من مخاطر الفضاء السيبراني

إن إستراتيجية الأمن السيبراني تُعد من أهم الاستراتيجيات الحساسة والمهمَة لحماية البُنية التحتية الحيوية الرقمية لأي مؤسسة، وبالتالي لا يمكن لهذه المؤسسات مهما كان نوعها أن تتجاهل اعتماد هذه الإستراتيجية ومهما كانت درجة تقدمها، فللأمن السيبراني دور كبير في حماية بيانات العملاء من مخاطر الفضاء السيبراني بوسائل تقنية، قانونية، تنظيمية، وأخرى بشرية، نتطرق إليها من خلال ثلاثة محاور كما يلي:

المطلب الأول: محاور إستراتيجية الأمن السيبراني

أولا: الجانب التقني (Technical Side):

يتعلق بمدى كفاءة الأجهزة والوسائل المستعملة، مع ضمان اليقظة للكشف والرَد على الهجمات السيبرانية من خلال ما يلي:[1]

– وجود بُنيات أساسية للبيانات والمعلومات الدقيقة والآمنة، تكون مضمونة، ومتوفرة، ومستمرة.

– توفر الأدوات والتقنيات لتحقيق الأمان كالتشفير، التوقيع، التصديق، جدار النار...إلخ، وقوة عامل الثقة في التطبيقات والخدمات المقدمة كالمعاملات المالية الرقمية، التجارية الإلكترونية، الصحة الإلكترونية، الحكومة الإلكترونية...الخ، وفعالية التدابير الموضوعة لحماية الحقوق، لا سيما فيما يتعلق بالتشفير وسرية البيانات.

–استخدام المعايير الدولية المعتمدة لوسائل الحماية ونظم إدارة المعلومات مثل الأيزو.

ثانيا: الجانب القانوني والتنظيمي (Legal and Regulatory Aspect):

يتعلق هذا الجانب بتعزيز وتحيين بصفة مستمرة ودائمة للأطر القانونية التي تضمن وتُؤمَن التطور المتعلق باستعمال تكنولوجيا المعلومات والاتصال، وكذا تأمين منظومات الإعلام بالإضافة إلى ضمان الفعالية والتناسق للأعمال الإلكترونية عن طريق تأطير مجموعة من الآليات الوظيفية والتنظيمية من خلال:

– أطر قانونية محيَنة ومناسبة لردع الجريمة السيبرانية.

– إدارة قوية وفعَالة لمواجهة المخاطر التقنية السيبرانية.

– تطبيق سياسات لخلق الثقة في الفضاء السيبراني.

ثالثا: جانب المورد البشري (Side of the Human Resource):

يتجلى نجاح مجال الأمن السيبراني بجاهزية وتكوين المورد البشري مع كفاءته العالية في الأجهزة والبرمجيات ونظم المعلومات والتقنيات وهندسة البنى التحتية والشبكات وتحكمه في الإنترنت ومواجهة الثغرات والتهديدات، مع وجود سلطات قضائية وشُرطية متمرَسة بالتكنولوجيا الجديدة والقادرة على التعاون مع نظيراتها في الخارج، بالإضافة إلى تحفيز ثقافة وطنية شاملة للأمن السيبراني.

الكفاءة والتكوين للعنصر البشري لوحدها لا تكفي، لذا يجب أيضا الترويج لثقافة الأمن السيبراني بما يتسق مع القرار رقم: 57/239 الخاص "بالجمعية العامة للأمم المتحدة المتضمن إرساء ثقافة عالمية للأمن السيبراني"،

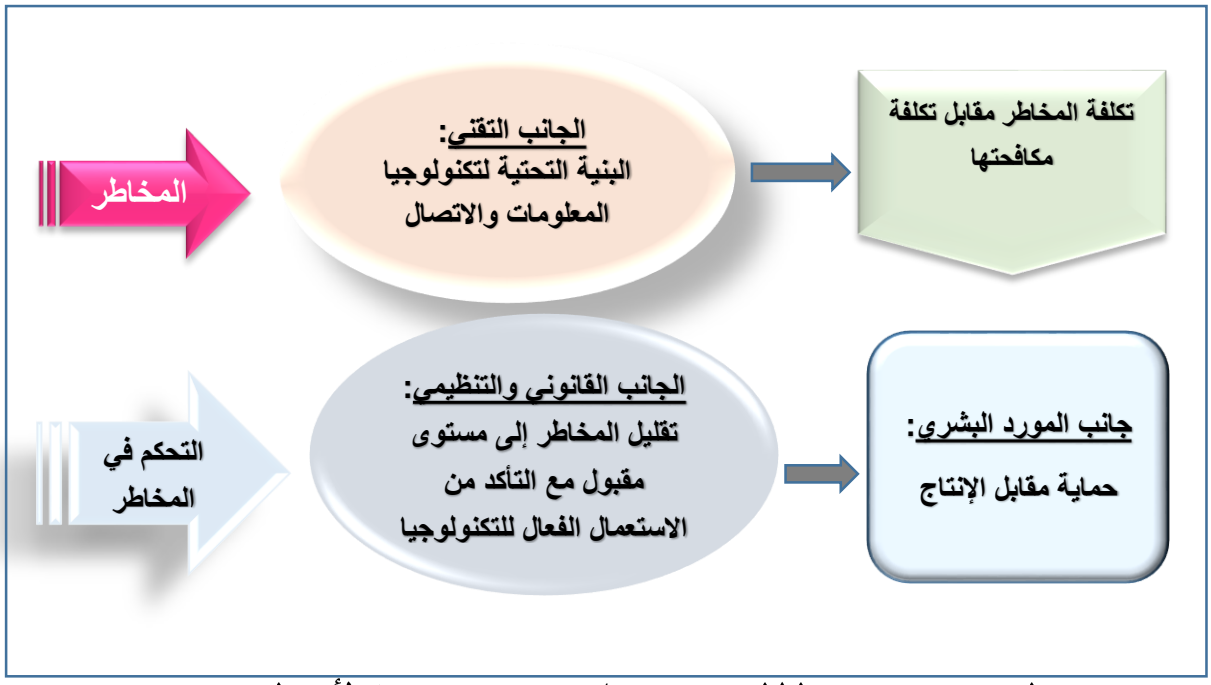
[1] وغرارة يوسف، **إستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبيري**، مجلة الدراسات الإفريقية وحوض النيل، العدد 3، المجلد الأول، المركز الديمقراطي العربي، برلين، ألمانيا، سبتمبر2018، ص 115.

وكذا القرار رقم: 58/199 المتعلق "بإرساء ثقافة عالمية لأمن الفضاء الحاسوبي وحماية البنى التحتية الحيوية للمعلومات".

مسألة الترويج لثقافة الأمن السيبراني ليست فقط محصورة بدور الحكومة في تأمين أنظمة التشغيل واستخدامات البنية التحتية للمعلومات، بما في ذلك الأنظمة التي تديرها الحكومة، ولكن أيضا بدورها المهم في توعية مؤسسات القطاع الخاص وأصحاب المصلحة والمجتمع، وبالمثل فإن هذا الدور أو العنصر يشمل تدريب مستعملي الأنظمة وإدخال تحسينات في المستقبل على الجوانب الأمنية، ومسائل أخرى هامة تشمل توفر السرية واحترام الخصوصية، إذا فلا ينبغي تناول مسألة الأمن السيبراني من منظور تقني تكنولوجي فحسب، ولكن ينبغي أن يشمل هذا المنظور عناصر من قبيل توعية المستخدمين نحو تعزيز ثقافة الأمن السيبراني.[1]

سيتم التطرق إلى محاور إستراتيجية الأمن السيبراني لدى المؤسسات الرقمية من خلال الشكل الموالي:

الشكل رقم (I–3): محاور إستراتيجية الأمن السيبراني لدى المؤسسات الرقمية



المصدر: من إعداد الطالب اعتمادا على محاور إستراتيجية الأمن السيبراني

يوضح الشكل أعلاه رقم (I–3): أن للأمن السيبراني ثلاثة محاور معتمدة في إستراتيجية حماية البيانات من مخاطر الفضاء السيبراني، ومن دون شك أن أي مؤسسة تقدم خدمات إلكترونية ومهما كان نوع نشاطها الرقمي فهي معرضة لمخاطر وتهديدات سيبرانية مختلفة، والواجهة الأولى لمواجهة هاته المخاطر هي الاعتماد على الجانب التقني والتكنولوجي بتوفر بُنية تحتية قوية وحديثة لتكنولوجيا المعلومات والاتصال، بمعنى آخر يجب

[1] رستم هاشم محمد، **جرائم الحاسب المستحدثة**، دار الكتب القانونية، مصر، الطبعة الأولى، 2015، ص 66.

توفير المورد المالي اللازم لاقتنائها وتوظيفيها، وبالرغم من ذلك لا يمكن الجزم بتوفر الحماية المطلقة، حيث أنه لما نتحدث عن الضرر الناجم عن الخطر فهذا يعني تكلفة إضافية للمؤسسة أو الشركة، ما يستدعي البحث عن عنصر آخر يُعزز الحماية التقنية، وهو العنصر الثاني الذي يتعلق بالجانب القانوني والتنظيمي المعتمد لتقليل المخاطر إلى مستوى مقبول، حيث أن الردع القانوني له انعكاسات إيجابية نحو مكافحة مثل هذه الجرائم والوقاية منها، أما الجانب التنظيمي فيتعلق بكل من التدابير والإجراءات اللازمة لتفادي حدوث المشاكل، والعنصر الثالث الأكثر أهمية هو الجانب البشري الذي يُفترض أن يتحلى بالجاهزية والتكوين والكفاءة العالية في الأجهزة التقنية والبرمجيات ونظم المعلومات ويتحكم في البنى التحتية والشبكات والإنترنت ومواجهة مختلف الثغرات الأمنية، وبحسب تحليل ورأي الطالب فإنه وبتكامل العناصر الثلاثة تكون لدى المؤسسة إستراتيجية أمنية سيبرانية شاملة مُحكمة وفعّالة.

المطلب الثاني: الوسائل التقنية لحماية البيانات في الفضاء السيبراني (Technical Means)

من أبسط أنواع وسائل الحماية المستخدمة كلمات السر، والوسائل البيولوجيّة كاستخدام البصمة ورفرفة العين، واستخدام المفاتيح المشفّرة كالأقفال الإلكترونية، ووضع برامج مضادة للفيروسات، ووضع أنظمة تكشف الاختراقات والثغرات الأمنية وتُعالجها، وعمل نسخ احتياطيّة للبيانات بعد الانتهاء من كل عمل، واستخدام أنظمة قويّة لتشفير البيانات، ونشر الوعي والثقافة السيبرانية بين المستخدمين لشبكة الإنترنت، فقد تكون كل هذه الوسائل من أجل ضمان عدم وصول أي شخص غير مصرح به إلى البيانات والمعلومات، فوسائل الحماية هذه وفّرت الكثير من الأمن للمؤسسات والشركات التي تعتمد على الإنترنت وعلى الأجهزة والأنظمة الإلكترونية، على سبلي المثال: البنوك وشركات الأموال والجامعات والمؤسسات الأمنيّة.

أ-التشفير (Encryption):

ما يسمى بـ(Codage) أو التعمية وهي: "العملية التي من خلالها يتم تغيير البيانات وجعلها في شكل غير مفهوم أو غير مقروء (أي تعميتها) (Inintelligibles). بحيث لا يستطيع إرجاعها إلى وضعها الأصلي إلا الشخص أو الأشخاص المصرح لهم فقط، الذين لديهم الأدوات اللازمة لذلك". وأما عن طريقة التشفير هي تحويل المعلومات إلى أرقام ورموز مختلفة يصعب فهمها من قبل الغير، حيث يكون ذلك باستخدام برامج خاصة لعملية التشفير أين تُحوَلها ضمن معادلة حسابية معينة، أما فهمها فيكون بامتلاك البرامج والرقم السري لها لإعادة المعلومات إلى طبيعتها، ويجري العمل بمثل هذه التقنية بأن يمتلك طرفا المعاملة برنامج خاص بالتشفير وفك التشفير،[1] حيث يتألف التشفير من عمليتين أساسيتين هما: التشفير، وفك التشفير، وحسب نوعية التشفير فإنه يمكن استخدام مفتاح تشفير أو أكثر لإتمام هاتين العمليتين، كما ينقسم التشفير إلى نوعين هما:

[1] حمودي فريدة، **نفس المرجع السابق**، ص 99.

-التشفير المتناظر (Symmetric Encryption).

-التشفير غير المتناظر، ويُسمى التشفير باستخدام المفتاح العام (Public Key Encryption).

وفيما يلي سنستعرض كل نوع من هذه الأنواع بشيء من التفصيل:

1-التشفير المتناظر: هو نظام تشفير يستخدم مفتاحا متناظرا لدى كل من المرسل والمستقبل، ويستخدم هذا المفتاح نفسه في عملتي التشفير وفك التشفير.

عملية التشفير: تشفر الرسالة الأصلية باستخدام خوارزمية التشفير* والمفتاح السري* للحصول عليها مشفرة.

عملية فك التشفير: (Decryption): هي "عملية إعادة تحويل البيانات إلى صيغتها الأصلية، من خلال استخدام المفتاح المناسب لفك الشفرة"،[1] حيث يفك تشفير الرسالة المشفرة باستخدام خوارزمية فك التشفير والمفتاح السري المشترك للحصول على الرسالة الأصلية.

إن قوة نظام التشفير (سواء أكان متناظرا، أم غير متناظر) تكمن في سرية المفتاح السري وقوته، وليس في إبقاء خوارزمية التشفير سرية، ومن المعروف ألَا تبقى الخوارزمية سرية وأن تكون معروفة حتى يمكن تطويرها من حين لآخر. ومن أجل الحصول على مفاتيح سَر قوية يمكن اتباع التعليمات الآتية:

- انتاج المفاتيح السرية بشكل آلي (أوتوماتيكي) من قبل النظام وليس من قبل المستخدم.
- استخدام مفاتيح سرية عشوائية مختلفة لكل عملية إرسال على حدى.
- استخدام مفاتيح سرية طويلة نوعا ما حيث لا تقل عن 256 بت (Bit).
-استخدام مفاتيح سرية في صيغتها الثنائية (0-1) فقط، وليس في صيغتها (الحروف والأرقام المعتادة).

2-التشفير غير المتناظر (التشفير باستخدام المفتاح العام): خلال سنوات مستمرة من البحث العلمي طُوَر التشفير المتناظر حتى تم إنتاج نظام التشفير القياسي المتقدم (AES)، الذي يعد آمنا لنقل بيانات مشفرة بمفتاح بطول لا يقل عن 256 بت (Bit)، لكن هناك مشكلة أساسية توجد في نظام التشفير المتناظر، هي كيفية الحصول على المفتاح نفسه لكل من المرسل والمستقبل، أو ما يسمى بمشكلة توزيع المفاتيح، ولحل هذه المشكلة جرى تطوير التشفير باستخدام المفتاح العام.

قدم التشفير باستخدام المفتاح العام طريقة حديثة تختلف تماما عن التشفير المتناظر، فهو تشفير غير متناظر أي لا يوجد مفتاح سري مشترك بين المرسل والمستقبل منذ البداية، وإنما يتم استخدام مفتاحان منفصلان،

---

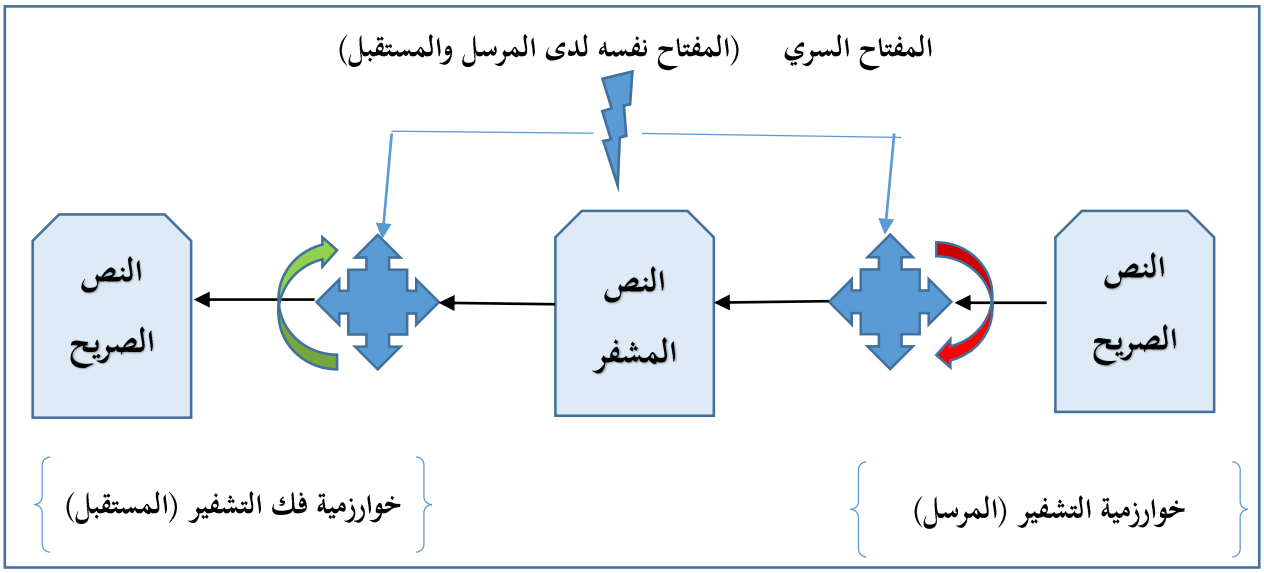
[1] محمد بن احمد السديري، **التجارة الإلكترونية تقنيات واستراتيجيات التطبيق**، 2023، على الموقع: http://faculty.ksu.edu.sa/mas/published%20papers/EC%20STRATEGY.pdf، تاريخ الاطلاع: 22-08-2023، الساعة: 21:00.

(*) خوارزمية التشفير (Encryption Algorithm): يعني مجموعة الخطوات والعمليات الرياضية التي يتم اتباعها لتحويل النص الصريح إلى نص مشفر.

(*) المفتاح السري (Key): هو عبارة عن قيمة غير معتمدة على الرسالة يختارها نظام التشفير أو المستخدم.

أحدهما يُستخدم للتشفير ويمكن الاطلاع عليه من قبل المستخدمين جميعا، والآخر لفك التشفير فلا يعرفه سوى المستقبل فقط.[1]

الشكل رقم (I-4): التشفير



المصدر: Christof Paar and Jan Pelzl، نفس المرجع السابق، ص 131.

يتضح من خلال الشكل رقم: (I-4)، أن عملية التشفير أو التعمية تتم من خلال تغيير البيانات أو النصوص وجعلها في شكل غير مفهوم أو غير مقروء، بحيث لا يستطيع إرجاعها إلى وضعها الأصلي إلا الشخص المرسل أو الشخص المستقبل أي المصرح لهم فقط، الذين لديهم الأدوات اللازمة لذلك باستعمال خوارزمية حسابية معينة تكون ضمن مفتاح خاص بهما.

ب-التصديق (التوقيع) الرقمي (Digital Authentication):

أحد أهم أدوات الأمن السيبراني الحديثة هو التصديق الرقمي (Digital Signature)، حيث يُعد وحدة بناء أساسية هدفها تحقيق عدد من عناصر الأمن السيبراني، كالتحقق من هوية أصل البيانات والمعلومات (Data Origin Authentication)، وكذا عدم الإنكار (Non-repudiation)، وكما هو معروف فعندما يوَقع الشخص المخوَل له بالتوقيع التقليدي أي اليدوي على رسالة ما أو خطاب معين، فإنه يُكسبه الصيغة الرسمية، أو بعبارة أخرى يتم التحقق من أصل هذه البيانات على أنها صدرت من الجهة أو الشخص المخول له بالتوقيع، ولذلك فإن أغلب الفقهاء جعلوا للتوقيع اهتماما كبيرا من خلال جعله الشرط الوحيد للمُحرر،[2] لكن عند استخدام التصديق الإلكتروني أو الرقمي فإن الأمر يختلف كثيرا، إذ أن التصديق الرقمي لا يكفي أن يكون مجرد

[1] Christof Paar and Jan Pelzl, **Understanding Cryptography**, Springer Verlag Berlin Heidelberg, 2010, P 133.

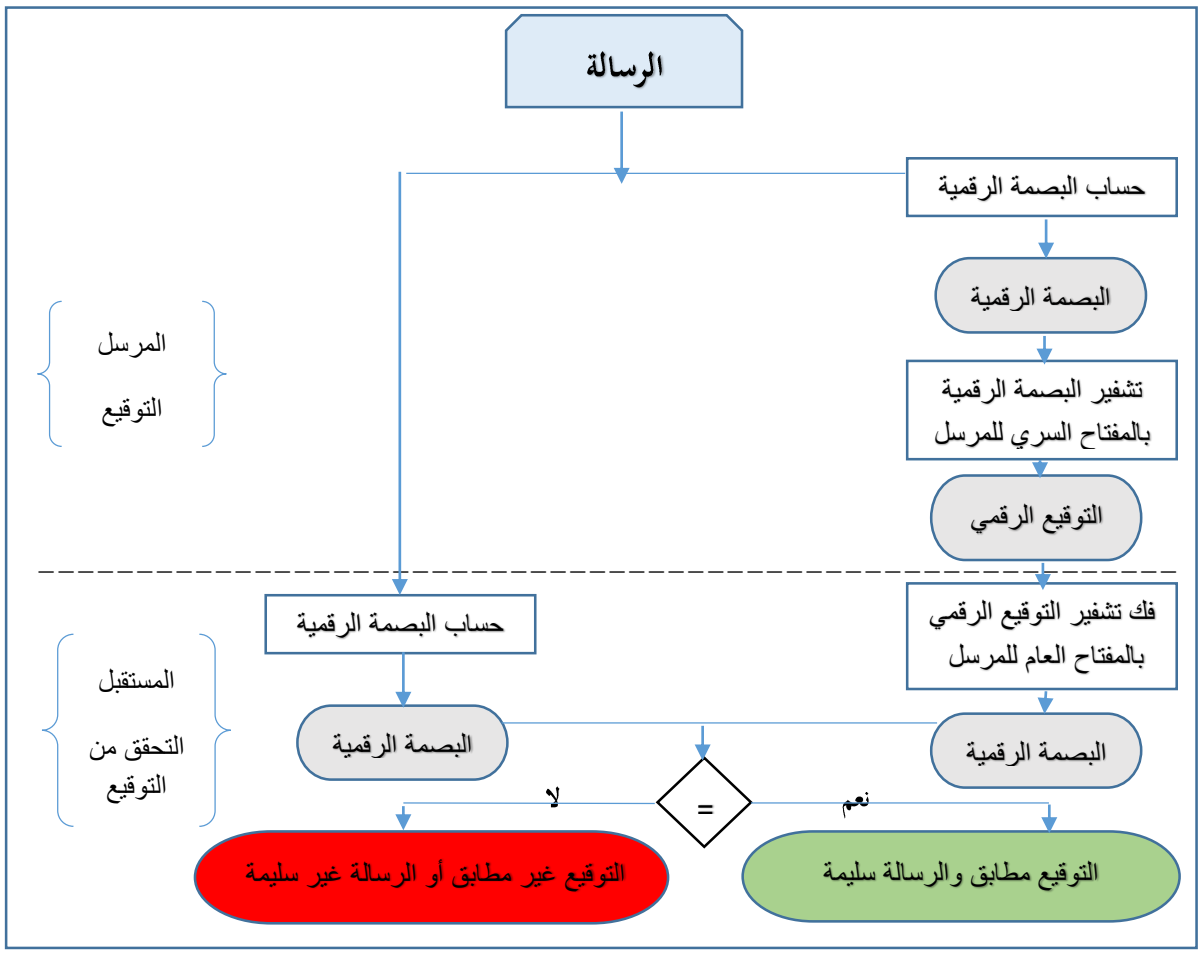
[2] علي عبد المحسن الجبوري، **الوسائل الحديثة للدفع في إطار التجارة الإلكترونية**، دار النهضة العربية، القاهرة، مصر، الطبعة الأولى، 2019، ص 166.

صورة التوقيع التقليدي فيتم لصقها بالرسالة، ففهي هذه الحالة من السهل نسخ هذا التوقيع والقيام بلصقه وإضافته لأي رسالة أخرى، لذلك فإن الأمر يتطلب أن يعتمد التصديق الرقمي بدُرة أو صيغة أساسية على الرسالة نفسها، بالإضافة إلى توقيع الشخص المخول له بالتصديق الرقمي من أجل إنتاج بصمة خاصة بكل رسالة (Message Digest)، ومن خلال هذه الطريقة يكون هناك بصمة فريدة ومختلفة لكل رسالة، ولا يمكن أن تنطبق بصمتان لرسالتين مختلفتين، حتى ولو صدرت من الشخص نفسه.

التصديق الرقمي يعتمد بشكل أساسي على نظام التشفير بالمفتاح العام، لكن بطريقة عكسية له، حيث يقوم معد الرسالة بالتوقيع عليها باستخدام مفتاحه السري (وليس المفتاح العام للمستقبل كما هو الحال في التشفير بالمفتاح العام)، على أن يقوم مستلم الرسالة بالتحقق من صحة التوقيع باستخدام المفتاح العام للموقّع، وهذا بهدف التحقق من صحة التوقيع وليس من أجل تشفير الرسالة كما هو الحال في التشفير بالمفتاح العام.

يوضح الشكل أدناه رقم: (I–5) مثال عن التوقيع الرقمي وإجراءات التحقق من صحته:

الشكل رقم (I–5): التوقيع الرقمي والتحقق من صحته



المصدر: نواف المنج، أمن المعلومات والشبكات، قسم الشبكات الكهربائية، مكتبة نور الرقمية، 2020، ص 164.

يتضح من خلال الشكل المبين أعلاه، أن التصديق الرقمي يتكون من عمليتين أساسيتين، هما كما يلي:

أ. **التوقيع (Sign)**: وهو عملية إجراء أو إنتاج التصديق الرقمي، ومدخلاتها هي: الرسالة والمفتاح السري للموقع، ونتيجتها هي التوقيع الرقمي، وهو رقم صحيح (طويل) (2048) بت (Bit) مثلا.

ب. **التحقق من صحة التوقيع (Verify)**: هي عملية التحقق من أن التوقيع تم من الشخص المعني على الرسالة المعنية، ومدخلاتها هي: الرسالة والمفتاح العام للموقع، ونتيجتها إحدى حالتين: إما مطابق، أو غير مطابق.

مما سبق يتضح أن المرسل لا يستطيع إنكار أنه أرسل هذه الرسالة، كونها وقَع عليها بمفتاحه السَري الذي لا يعرفه أحد ولا يملكه سواه، وكذلك فإن البصمة الرقمية للرسالة هي قد ضمنت سلامة الرسالة الأصلية من حيث كشف أي حذف أو تعديل أو إضافة تم عليها.

وبذلك يمكننا أن نستخلص ما يلي:

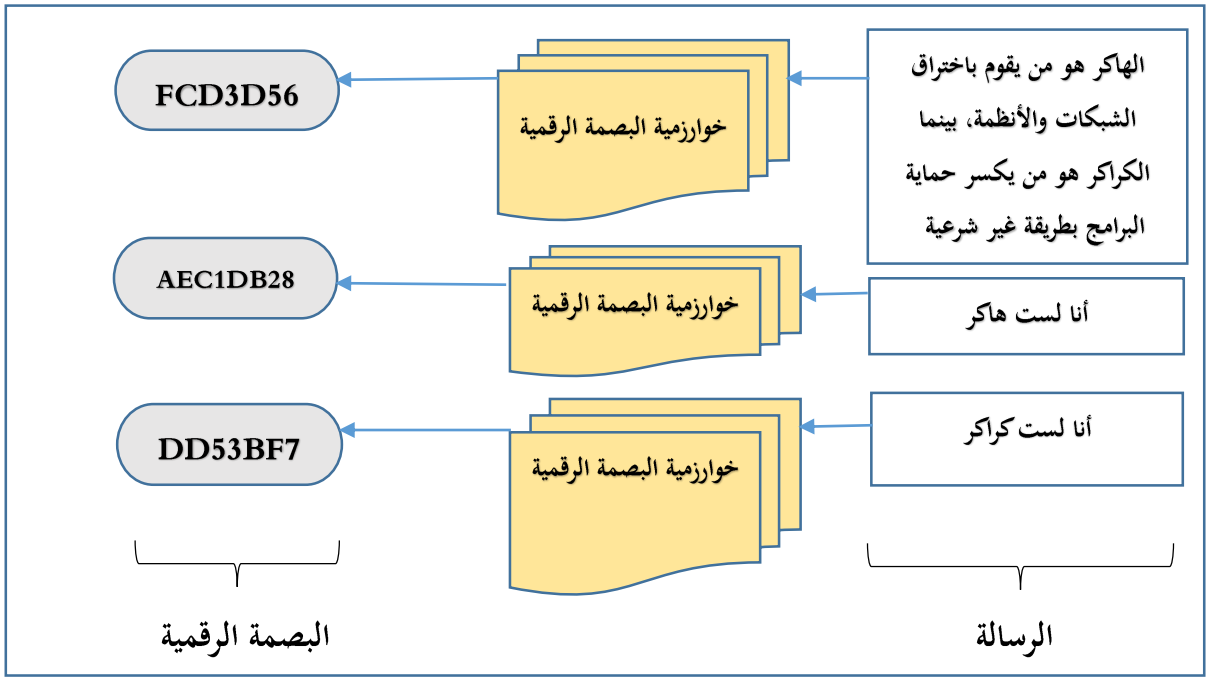
- ✓ التوقيع الرقمي هو التزام من الموقع بما ورد في الوثيقة.
- ✓ التوقيع الرقمي ليست كما يعتقد البعض بأنه ما هو إلا توقيع باليد ولكنه مصور رقميا، ولو كان كذلك لأصبح بإمكان أي شخص أن يصور أي توقيع ويدعي بأنه صاحب هذا التوقيع.
- ✓ هو شهادة رقمية تصدر عن أحد الهيئات المستقلة فتُميَز كل مستخدم عن الآخر.
- ✓ يمكن استخدامه في إرسال أي وثيقة أو إقرار أو عقد أو تعهد، ويُعتبر قانوني.
- ✓ العقود والوثائق التجارية المذيَلة بالتوقيع الرقمي هي لا تحتاج إلى المصادقة من كاتب عدل أو أي جهة أخرى، لأنها صادرة أساسا من جهة معترف بها.

ج-البصمة الرقمية (Hash Value):

على الرغم من وجود عدة تطبيقات مهمة للبصمة الرقمية، إلا أن أشهرها هو استخدامها في التصديق الرقمي، فعادة ما تكون الرسالة طويلة، قد يصل طول بعضها إلى مئات الصفحات، وهذا ما يجعل تطبيق التصديق الرقمي عليها صعبا جدا، ومن هنا جاءت البصمة الرقمية لتحُل مشكلة التعامل مع الرسائل الطويلة.

فالبصمة الرقمية هي: "سلسلة قصيرة وثابتة الطول من البتَات* (Byte) تُشكل بصمة فريدة لكل رسالة"، ويعنى ذلك أن يكون لدينا لكل رسالة بصمة رقمية مختلفة، لكن جميع البصمات يكون طولها واحد مكوَن من العدد نفسه من البتَات، 160 بت مثلا، مهما كان طول الرسالة، (فالبتَات **(Byte)**: هي وحدة معلومات رقمية في الحاسوب وفي الاتصالات، في العادة تتكون من ثمانية بت وهو إما الصفر أو الواحد في الحاسوب). ويوضح الشكل رقم: (07) مثال لبعض الرسائل وبصماتها الرقمية:

الشكل رقم (I-6): بعض الرسائل وبصماتها الرقمية



المصدر: نواف المنج، أمن المعلومات والشبكات، قسم الشبكات الكهربائية، مكتبة نور الرقمية، 2020، ص 167.

نلاحظ في الشكل رقم: (I-6) أن لكل رسالة بصمة رقمية مختلفة، لكن جميعها بطول (32) بت (ثمانية خانات بالتمثيل السّت عشري كل واحد منها أربعة بتات)، ومن أهم ما يُميز البصمات الرقمية أن أي تعديل في الرسالة ولو كان بسيطا جدا ينتُج عنه تغيير كبير في البصمة الرقمية، وهذا واضح في الرسالتين الثانية والثالثة من خلال بصماتها الرقمية حسب الشكل، حيث أن الفرق بينهما هو حرفان فقط (ك، ر)، لكن الفرق بين بصمتيهما كبير جدا.

البصمة الرقمية تُحسب باستخدام خوارزميات خاصة بذلك، حيث يتم الحصول من خلالها على بصمة رقمية فريدة خاصة بكل رسالة، ومن أشهرها: خوارزمية (SHA-2)، كما يوجد خوارزمية حديثة تحت التجربة والتصميم يتوقع أن تُقنن لتصبح قياسية عالمية وهي (SHA-3).

بما أن البصمة الرقمية تُظهر بوضوح أي تغيير ولو كان بسيطا جدا على الرسالة الأصلية، فإنه يمكن من خلال ذلك كشف أي تعديل أو إضافة أو حذف على الرسالة الأصلية، ومعنى ذلك أنه حين الاتصال بالإنترنت فالبصمة الرقمية تترك علامة أو أثر لا يمكن محوه من الفضاء الإلكتروني.

د-جدار النار (Faire Wall):

عندما تكون شبكة الاتصالات الداخلية الخاصة بالمنشأة متصلة بشبكة الإنترنت، أو أي شبكة خارجية، فإن هناك طريقتين للاتصال: أحداها يصل من الخارج إلى شبكة المنشأة، أما الآخر من شبكة المنشأة إلى الخارج، ولمنع أي اختراق أو تطفل وأي وصول غير مصرح به لشبكة المنشأة، يجب استخدام أداة تمنع ذلك

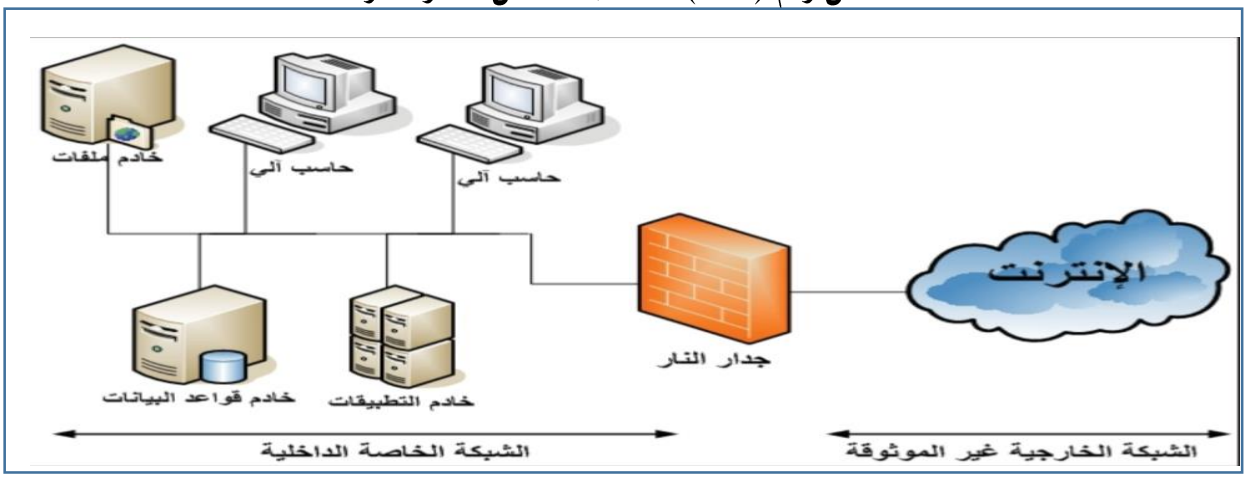
هذه الأخيرة تُسمى "جدار النار" أو "جدار الحماية"، فجدار النار إما أن يكون جاهزا مستقلا خاصا يُصنع لهذا الغرض وبه برامجه الخاصة به، أو يكون برنامجا يُرَكَب على أجهزة الحاسب الآلي العادية.

من هنا يمكن تعريف جدار النار على أنه: "نظام أو مجموعة من الأنظمة تعمل على تقوية السيطرة إلى الوصول عند استخدامها كجدار ما بين إثنين من شبكات العمل، وغالبا ما يستخدم لعمل حدود ما بين الإنترنت الداخلي الخاص بالشركة مع الإنترنت.[1]

حيث ظهرت تقنية الجدار الناري في أواخر سنة 1988 م، عندما قام مهندسون بتنظيم نظام فلترة العبوة، ليتم تعريفه باسم جدار النار،[2] فكبرى المؤسسات والشركات العالمية المعروفة مثل: IBM وMicrosoft هي تستخدم جدار النار عندما تقوم بتشغيل مواقع الويب، وكذا حين استضافة المواقع ومزودي خدمات الإنترنت ISPs.[3]

يعمل جدار النار كمنقّح أو مصفَ لرُزم (Packets) البيانات الداخلة لشبكة المنشأة والخارجة منها، أي أنه يكوَن طبقة عازلة بين العالم الخارجي وشبكة المنشأة، كما تمر جميع رزم البيانات الداخلة والخارجة من شبكة المنشأة عبر جدار النار ليقوم بتصفيتها ويسمح بمرور الرزم أو الأنشطة المصرح لها فقط، هذه التصفية تكون من خلال عدة أشكال، فإما على أساس نوع البيانات مثلا قد يمنع مرور أي رزم ذات النوع الناقل للملفات (ETP)، أو تكون على أساس التاريخ والوقت والنوع، مثلا قد يمنع مرور أي رزم من نوع (HTTP) في أوقات الدوام الرسمي للمنشأة، وأيضا تكون على أساس أي تصفية أخرى بحسب الحاجة.[4]

الشكل رقم (I-7): أساسيات عمل جدار النار



المصدر: Raphael Grevisse Yende، نفس المرجع السابق، ص 77.

[1] ذيب بن عايض القحطاني، **نفس المرجع السابق**، ص 108.

[2] حوالف عبد الصمد، **النظام القانوني لوسائل الدفع في الجزائر، دراسة مقارنة**، دار الجامعة الجديدة، الإسكندرية، مصر، 2016، ص 578.

[3] **تقنيات التجارة الإلكترونية**، على الموقع: http://ecommercetechnology.org/data/88.htm. تاريخ الاطلاع:14-08-2023، الساعة: 08:00.

[4] Raphael Grevisse Yende, **Support de Cours de Sécurité Informatique et Crypto**, Congo Kinshasa, 2018, P 68, https://hal.science/cel-01965300/document, Retrieved: 13-04-2022, 20:10.

يوضح الشكل رقم: (I-7) كيفية عزل أجهزة الخوادم الرئيسية عن الشبكة الداخلية، وهذا ما يساعد في حماية الأجهزة من أخطاء المستخدمين أو من رُزم البيانات الداخلية الضارة، حيث توضح الدراسات الحديثة أنه ما بين: (70-80%) من المخاطر التي تتعرض لها الأجهزة يكون سببها المستخدمين الداخليين الذين عادة ما يكون لهم صلاحية الدخول إليها.

هنا تظهر جليا أهمية جدار النار، حيث أن لديه القدرة على تصفية مختلف رُزم البيانات القادمة من المستخدمين المصرح لهم، وكذا ومنع الرُزم التي تحمل خطر على الأجهزة الرئيسية أو المعلومات الهامة، كما تظهر هنا أيضا أهمية عمل التهيئة والتعريفات اللازمة لجدار النار بالشكل الصحيح، وإلا سيؤدي ذلك إلى بروز ثغرات أمنية مختلفة، ومن المعروف أن عمل تهيئة خاطئة لجدار النار يكون له أثر سلبي أكثر مما لو لم يكن هناك جدار نار أساسا، كون ذلك يكون بمنزلة تضليل لمديري شبكات الاتصال بالاعتماد على جدار النار، بينما في الحقيقة هو لا يقدم الحماية الكافية، أو بعبارة أخرى يُعطي حسا أمنيا خاطئا.

جدار النار يعتمد في عمله على جداول الفلترة أو التنقيح التي يتم تخزينها داخل جدار النار، كما يسمح لرُزم البيانات بالمرور من عدمه إلا بعد الرجوع لهذه الجداول لمعرفة الرُزم المسموح بها، وكذا الرزم غير المسموح بها.

كما تجدر الإشارة، إلى ضرورة عدم الاعتماد على جدار النار لوحده لعمل الحماية الكاملة للشبكات، كون جدار النار لا يقوم بالحماية الكاملة لكل شيء، على سبيل المثال: استخدام جدار النار لا يُلغي إطلاقا الحاجة إلى استخدام برامج مكافحة الفيروسات.

ذ-البرامج المضادة للاعتداءات الإلكترونية (Programs):

هذه البرامج تُعرف أيضا باسم الكيان البرمجي فهي مجموعة أو سلسلة من الأوامر والتعليمات التي تتحكم وتُشرف على منظومة الشبكات والحواسيب، وهي عبارة عن إجراء حمائي منها ما هو على مستوى الفرد، ومنها ما هو على مستوى المؤسسات والشركات، ومنها ما هو على مستوى أجهزة الدولة،[1] وفي بحثنا هذا سنتناول في الجانب التطبيقي المستوى الثاني المتعلق بالإجراء الحمائي بواسطة البرامج المضادة للاعتداء الإلكتروني على البنوك.

فالعديد من البنوك قامت بتطبيق برنامج الشبكة العصبية، الذي هو أحد برامج الكمبيوتر إذ يقوم بمراقبة كافة العمليات التي تتم باستخدام البطاقات الإلكترونية الخاصة بالبنك سواء الممغنطة أو الذكية، كما يقوم باكتشاف العمليات الإلكترونية المشبوهة، بالإضافة إلى اعتماد البنوك على العديد من البرامج الفعّالة الخاصة بالشبكات والحواسيب مثل: برنامج تقنية الطبقات الأمنية SSL المسمى بـ: Netscape، برنامج الحركات المالية الآمنة SET، برنامج Alert 99 Internet، برنامج Down Lock، برنامج الفتحات الآمنة SLL، مضادات

[1] طارق إبراهيم الدسوقي عطية، **الأمن المعلوماتي**، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، 2015، ص 581.

الاعتداء Macafee، PcCline، Norton antivirus، موجهات (الراوتر) وأجهزة منع الدخلاء (IPS)،...إلخ.

ر-تقنية البلوكشين في مجال الأمن السيبراني للمعاملات المالية الإلكترونية:

يقوم العملاء كل يوم بإتمام الكثير من عمليات تحويل الأموال أو خدمات البيع والشراء عبر الإنترنت وغيرها الكثير من المعاملات التي تجعلهم يشاركون معلوماتهم المالية والشخصية عبر الشبكة العنكبوتية، ولكن رغم كل هذه الخدمات السريعة والمريحة فهي محفوفة بمخاطر وثغرات مختلفة في بروتوكولات الأمان، ما يعرض المستخدمين وخصوصيتهم للخطر، الأمر الذي جعل شركات تكنولوجيا المعلومات وخبراء الأمن يعملون بجهد على إيجاد حلول لحماية المستخدمين، حتى توصلوا إلى استخدام تقنية البلوكشين "blockchain" التي تعد سلاج جديد في مجال الأمن السيبراني للمعاملات المالية الإلكترونية.

مفهوم تقنية البلوكشين:

هي تقنية حديثة تقوم على تسجيل البيانات عبر سجلات بطريقة مشفرة بشكل لا مركزي يمكن أن تكون البيانات شيئا ملموسا (منزل، مسكن، نقود، أرض) أو غير ملموس (ملكية فكرية، براءة اختراع، حقوق نشر، علامة تجارية)، حيث تكون هذه السجلات مرتبطة ببعضها البعض بواسطة تقنيات تشفير معقدة غير قابلة للاختراق نظرا لارتباط كل سجل بمفتاح خاص، يتم تخزينها على عدد هائل من أجهزة الكمبيوتر حول العالم.[1]

كما تعرف على أنه "برنامج معلوماتي مشفر يتولى مهمة سجل موحد للمعاملات على الشبكة فكل مجموعة من المعاملات مرتبطة بسلسلة ما، يمنح المشاركين صورة شاملة عن كل ما يحصل في المنظومة بأكملها".[2]

كما عرفها قانون ولاية إلينوي بشأن تقنية البلوكشين الذي دخل حيز النفاذ في 01-01-2020 بأنها "سجل إلكتروني تم إنشاؤه بواسطة استخدام طريقة لا مركزية من قبل أطراف متعددة، للتحقق من سجل رقمي للمعاملات وتخزينه، ويجري تأمينه عن طريق استخدام الهاش الخاص بمعلومات المعاملة السابقة".[3]

مكونات البلوكشين:

تتكون كل سلسلة من سلاسل البلوكشين من كتل block متعددة وكل كتلة لها ثلاثة عناصر أساسية:

- البيانات التي تم تسجيلها في الكتلة block.

---

[1] الموقع: https://t8t.in/%D8%AA%D9%82%D9%86%D9%8A%D8%A9، تاريخ الاطلاع: 06-02-2024، على الساعة: 10:00.

[2] قادري نور الهدى، مكلكل بوزيان، **التشفير بتقنية البلوك تشين ودوره في حماية المعاملات الإلكترونية**، مجلة القانون العام الجزائري والمقارن، المجلد 08، العدد 02، ديسمبر 2022، ص 566.

[3] هيثم السيد أحمد عيسى، **نشأة العقود الذكية في عصر البلوكشن**، دار النهضة العربية للنشر والتوزيع، القاهرة، الطبعة الأولى، 2021، ص 16.

- 32 بايت من الأرقام تنشأ عشوائيا فور إنشاء الكتلة block ويطلق عليها اسم nonce والتي سيتم بعد ذلك تشفيرها إلى أرقام hash.
- مفتاح التشفير hash عبارة عن رقم 256 بت مضمن في nonce، يجب أن يبدأ بعدد كبير من الأصفار أي أن تكون صغيرة للغاية.

كيفية عمل البلوكشين:

1-عند حدوث أي معاملة يتم تسجيلها على أنها كتلة من البيانات.

2-كل كتلة متصلة بكتلة قبلها وبعدها حيث تشكل هذه الكتل سلسلة من البيانات، فعندما ينتقل الأصل من مكان إلى آخر أو تتغير الملكية توثق الكتل الوقت الدقيق وتسلسل المعاملات، وترتبط الكتل معا بشكل آمن لمنع أي كتلة من التغيير أو إدراج كتلة بين كتلتين موجودتين، فهي تعتمد على التشفير الذي هو عبارة عن خوارزميات تحول البيانات التي تم إدخالها في الكتلة.

3-يتم جمع معلومات المعاملات معا في سلسلة لا يمكن التعديل عليها، تعمل كل كتلة إضافية على تعزيز التحقق من الكتلة السابقة وبالتالي تتكون البلوكشين بالكامل، هذا يجعلها غير قابلة للعبث بها ويزيل إمكانية حدوث أي تزوير ويبني سجلات موثوقة يمكن لأعضاء الشبكة الاعتماد عليها.

4-البلوك شين هي دفتر للمعاملات لا مركزي، ولا تتحكم في جهة واحدة مركزية يتعين الرجوع إليها للوصول إلى محتوى الدفتر أو التفاعل معه، وإنما يتم حفظ نسخة من البيانات لدى المشتركين في شبكة البلوكشين، وأيي تعديل يحدث على هذه الأخيرة يضاف بشكل متزامن لدى الجميع، فليس هناك جهة واحدة تحتفظ بالبيانات.[1]

من خلال ما سبق ذكره، وبالرغم من توفر وسائل الحماية الفنية أو التقنية، إلا أنها لا تكفي وحدها لحماية بيانات ومعلومات المنشأة، الأمر الذي يدعونا إلى البحث عن إمكانية إضفاء هذه الحماية عن طريق آليات إضافية أخرى تتمثل في القانون والقضاء، والعنصر البشري الكفىء، وهذا ما سنتطرق إليه أيضا:

المطلب الثالث: الوسائل القانونية لحماية البيانات في الفضاء السيبراني (Legal Means)

كون الجزائر لا تملك تقنينا مصرفيا مستقلا يُوحَد ويشمل كل الأحكام المتعلقة بهذا الجانب من المعاملات الإلكترونية، جاءت النُصوص القانونية المتعلقة بالأمن السيبراني مُبعثرة بين القوانين المختلفة وأنظمة بنك الجزائر، وفي سياق الأمن السيبراني للمعاملات الإلكترونية، والتي قصد المشرع الجزائري من خلالها الحماية القانونية للبيانات والمعلومات الإلكترونية، قام هذا الأخير في السنوات الأخيرة بتدارك نسبي للفراغ القانوني والقصور التشريعي الواضح في مجال الجريمة الإلكترونية، حيث تمخَض عنه إصدار عدة قوانين للمواجهة الفعَالة الرادعة

[1] أنس محمد عبد الغفار سلامة، **إثبات التعاقد عبر تقنية البلوك تشين**، مجلة العلوم القانونية والاجتماعية، المجلد 05، العدد 02، جوان 2020، ص 65.

للنشاط الإجرامي المنتهك لمختلف نظم أمن المعلومات والبيانات، حيث أخص المشرع الجزائري تنظيم الجرائم السيبرانية بقوانين **عامة** وأخرى **خاصة**، فتمثلت القوانين "**العامة**" فيما يلي:

أولا: الوسائل القانونية العامة:

الوسائل القانونية العامة تتضمن قوانين محلية وأخرى دولية، نتطرق إليها بالتفصيل كما يلي:

1- الوسائل القانونية المحلية:

- **الدستور الجزائري**: كفل دستور 1996 وكذا التعديلات الطارئة عليه سنة 2016، و2008، و2020، حماية الحقوق الأساسية والحريات الفردية، وذلك عن طريق أهم المبادئ الدستورية في مواده:

المادة 38: الحريات الأساسية وحقوق الإنسان والمواطن هي مضمونة.

المادة 44: حرية الابتكار الفكري والفني والعلمي مضمونة للمواطن، وحقوق المؤلف يحميها القانون.

- **القانون الجنائي**: حصر الإجرام السيبراني بتحديد كل الأفعال غير المشروعة التي تُعد من قبيل الجريمة السيبرانية، هي تنطبق أيضا على تلك التصرفات والأفعال التي توصف على أنها جرائم مرتكبة عن طريق تكنولوجيا المعلومات والاتصال.

- **قانون العقوبات**: استدرك نسبيًا المشرع الجزائري في السنوات الأخيرة الفراغ القانوني في مجال الجريمة السيبرانية، حيث تمخض عنه إصدار القانون: 04-15، المتضمن تعديل قانون العقوبات، وذلك بتخصيص الفصل السابع مكرر للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات،[1] ليصدر في: 05 أوت 2009 القانون رقم:04-09، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها،[2] حيث جاء في فصله الخامس على إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحته، مهامها تنشيط عمل السلطات المكلَفة بمكافحة الجرائم ذات الصلة بتكنولوجيا الاعلام والاتصال،[3] كما قام المشرع بتعديل المواد التالية: 303-333-394-396 من قانون العقوبات، المتضمنة تجريم وتسليط العقاب على كل من يثبُت في حقه اختراق أنظمة معلومات المؤسسات أو الأفراد بطريقة غير شرعية، كما جاءت المادة: 87 من نفس القانون صريحة في تجريم وتسليط العقاب على كل من يثبُت تورطه في أعمال الإشادة والتجنيد لصالح الجماعات الإرهابية نقصد الإرهاب الإلكتروني.

إضافة إلى ذلك أصدر رئيس الجمهورية مرسوم رئاسي تحت رقم: 261-15، مؤرخ في: 8 أكتوبر 2015، من خلاله يُحدد تشكيلة وتنظيم وكيفيات سير هاته الهيئة الوطنية لمكافحة الجرائم ذات الصلة بتكنولوجيا الاعلام

---

[1] القانون رقم: 04-15 المتضمن **الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات**، المتمم للأمر رقم: 66-156 المتضمن لقانون العقوبات الصادر بتاريخ: 05-11-2004، ج.ر.ج.ج، عدد 71.

[2] القانون رقم 04-09 المتضمن **القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها**، ج.ر.ج.ج، عدد 4.

[3] مليكة درياد، **المساس بأنظمة المعالجة الآلية للمعطيات**، مجلة حوليات، جامعة الجزائر 1، العدد 33، الجزء الأول، مارس 2019، ص 244.

والاتصال، أيضا شمل التشريع بعض المجالات التي يُحتمل أن تشملها الجريمة الإلكترونية والتي لها صلة بمجال الحريات الخاصة على غرار قانون الملكية الفكرية، الثقافية، حقوق المؤلف.[1]

- **قانون الإجراءات:** تطرق المشرع الجزائري إلى الإجراءات التي يجب اتخاذها على الصعيد الوطني، والتي تخدُم التحريات الجنائية التي تُرتكب عن طريق المنظومة المعلوماتية، وجمع الأدلة ذات الطابع الإلكتروني، بالرغم من وجود صعوبات عدة في مجال مكافحة الإجرام السيبراني مثلا: تحديد هوية مرتكب الجريمة، وكذا ضياع البيانات الإلكترونية التي يمكن تعديلها او نقلها أو محوها في ثواني معدودة، فمثلاً يستطيع الشخص الذي يتحكم في البيانات أن يستغل الثغرات الأمنية في أي منظومة معلوماتية ليقوم بمحو البيانات مدمراً بذلك جميع الأدلة التي يقوم عليها التحقيق الجنائي، لذا تُعتبر السرية والسرعة من المكونات الأساسية لنجاح التحريات.

وتعزيزا لقانون الإجراءات الجزائية تدعَمت الإجراءات القانونية بآليات فنية جديدة تتمثل في صدور القانون رقم: 03-16، المؤرخ في: 19-06-2016، المتضمن البصمات الجنائية في الإجراءات الجزائية لتحديد هوية الأشخاص، وتعزيز الجهات القضائية بأربعة محاكم خاصة متواجدةب: (الجزائر، وهران، قسنطينة، ورقلة)، لتسهيل التحريات والبحث لذوي الاختصاص من الأجهزة الأمنية والبَث في القضايا المعروضة دون الرجوع إلى الوصاية، بالإضافة إلى ذلك زيادة تمديد قطاع الاختصاص المحلي لوكيل الجمهورية في الجرائم الإلكترونية من خلال المادة رقم: 37 من قانون الإجراءات الجزائية،[2] إضافة الى ذلك صدور الامر رقم: 11-21، المؤرخ في: 25 أوت 2021، المتضمن تعديل قانون الإجراءات الجزائية، هذا النص القانوني رقم: 155-66 تعلق باستحداث القطب الجزائي استحداث القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الاعلام والاتصال.[3]

ثانيا: القوانين الخاصة :

تتمثل القوانين "**الخاصة**" التي أقرَها المشرع الجزائري في مجال الجريمة السيبرانية فيما يلي:

- **القانون الخاص بالبريد والاتصالات الإلكترونية:** لقد جاء القانون رقم: 04-18، المؤرخ في: 24 شعبان 1939 ه الموافقـل: 10-05-2018،[4] الذي يُحدد القواعد العامة المتعلقة بالبريد والاتصالات

---

[1] جمال بوزادية، **الإستراتيجية الجزائرية في مواجهة الجرائم السيبرانية الآفاق والتحديات**، مجلة العلوم القانونية والسياسية الجزائر، المجلد 10، العدد 01، أفريل 2019، ص17.

[2] القانون رقم: 03-16، المتضمن **البصمات الجنائية في الإجراءات الجزائية لتحديد هوية الأشخاص وتعزيز الجهات القضائية بأربعة محاكم خاصة**، الصادر بتاريخ: 2016/06/19.

[3] الأمر رقم: 11-21، المتضمن **قانون الإجراءات الجزائية، استحداث القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الاعلام**، المؤرخ في: 25 أوت 2021.

[4] القانون رقم: 04-18، المؤرخ في: 10-05-2018 الذي **يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية**، ج.ر.ج.ج، عدد 27، صادر بتاريخ 27 شعبان عام 1439 ه الموافق ل 13 ماي 2018.

الإلكترونية، حيث جاء في المادة رقم: 04 أنه: "تسهر الدولة في إطار الصلاحيات المرتبطة بمهامها خصوصا على ما يأتي:

-تحديد وتطبيق معايير إنشاء واستغلال مختلف الخدمات الإلكترونية.

-أمن وسلامة شبكات الاتصالات الإلكترونية.

-استمرارية وانتظام الخدمات المقدمة للجمهور، ...إلخ

ركزت هذه المادة على أمن وسلامة شبكات الاتصالات الإلكترونية، دون التفصيل في أحكام الأمن السيبراني.

- **قانون التأمينات:** نص قانون التأمينات على تنظيم الجريمة الإلكترونية، من خلال مؤسسات وهيئات الضمان الاجتماعي، وذلك في عدة نصوص تخص البطاقة الإلكترونية.

- **قانون التجارة الإلكترونية:** صدر قانون التجارة الإلكترونية في الجزائر بموجب القانون رقم: 05-18، مؤرخ في: 24 شعبان عام 1439، الموافقـ: 10 ماي 2018، المتضمن قانون التجارة الإلكترونية،[1] حمل في طياته مواد قانونية متعلقة بالتجارة الإلكترونية، حيث نصت المادة رقم: 29 منه على أنه: "تخضع منصات الدفع الإلكترونية المنشأة والمستغلة طبقا للمادة رقم: 27 أعلاه، لرقابة بنك الجزائر، وهذا لضمان استجابتها لمتطلبات التشغيل البيني، وسرية البيانات، وسلامتها، وأمن تبادلها"، وقد أقر مجموعة من المحددات التشريعية والشروط المنظمة لممارسة هذا النوع من التجارة بهدف حماية العملاء وبياناتهم، ومن أهم هذه الشروط هي:

- يجب على التاجر تسجيل المتجر الإلكتروني في السجل التجاري الوطني، أو في سجل الصناعات الحرفية والتقليدية وهذا حسب طبيعة المتجر.
- يجب أن يكون الموقع الإلكتروني للمتجر يحمل نطاق .com.dz.
- يجب أن يحتوي الموقع الإلكتروني على الأدوات التي تسمح للعملاء بالتأكد من صحته وأمانه.
- كل عملية بيع وشراء تتم عن بعد، يجب أن تكون موثقة بعقد إلكتروني يُصادق عليه بشكل إلكتروني.
- يجب على صاحب المتجر الإلكتروني عرض العقد التجاري على الموقع بطريق واضحة ومقروءة.[2]

- **نظام بنك الجزائر:** تُعتبر النصوص القانونية لأنظمة بنك الجزائر من بين النصوص التي تناولت مسألة الأمن السيبراني، حيث صدر سنة 2005، نظام رقم: 07-05، مؤرخ في: 28 ديسمبر 2005، المتضمن أمن أنظمة الدفع، ونصت المادة الأولى منه على ما يلي: "يهدف هذا النظام إلى تعريف أنظمة الدفع وجهاز الأمن الخاص بها"[3] ، فقد جاء هذا القانون ليُحدد أنظمة الدفع فيما بين البنوك وجهاز الأمن الخاص بها، وجاءت

[1] قانون التجارة الإلكترونية في الجزائر الصادر بموجب القانون: 05-18، المتضمن **قانون التجارة الإلكترونية**، المؤرخ في 24 شعبان عام 1439 الموافق 10 ماي سنة 2018.

[2] موقع التجارة الإلكتروني: https://www.commerce.gov.dz، تاريخ الاطلاع: 01-08-2023، على الساعة: 10:40.

[3] قانون بنك الجزائر رقم 07-05 المؤرخ في 28-12-2005، المتضمن **أمن أنظمة الدفع**، ج.ر.ج.ج، عدد 37، الصادر بتاريخ: 04-06-2006.

المادة الرابعة فقرة أولى منه على أنه: "يتضمن أمن أنظمة الدفع أمن البنية الأساسية لأنظمة الدفع وكذا أمن الوسائل الدفع..."، فحسب هذه المادة فإن أمن أنظمة الدفع يتضمن أمن البنية الأساسية لها (وتتمثل أنظمة الدفع في الجزائر في نظام التسوية الفورية للمبالغ الكبيرة ARTS، ونظام الدفع المستعجل ATCI)، وكذا أمن وسائل الدفع الإلكترونية المتمثلة في: البطاقات البنكية بكل أنواعها والتحويلات المصرفية الإلكترونية.

ولقد جاءت الفقرة الثالثة من المادة رقم: 4 من النظام السالف الذكر، حيث نصَت على: "تُلقى مسؤولية وضع أجهزة أمن أنظمة الدفع على عاتق مُسيريها والمشاركين في هذه الأنظمة، بينما يسهر بنك الجزائر على الاشتغال الحسن لهذه الأنظمة وأمنها"، وما نستشفه من نص هذه المادة أن مختلف المسيرين والمشاركين في أنظمة الدفع هم المسؤولين على وضع أجهزة أنظمة الدفع، ويتكفل بنك الجزائر بصفته بنك البنوك بمراقبة الاشتغال الحسن لهذه الأنظمة ويضمن أمنها، كما يشمل أمن البنية الأساسية لأنظمة الدفع: توفر الأنظمة، السرية وقابلية المراجعة، صحة المعلومات المتبادلة، رسم مخطط المعطيات المتبادلة، ويدخل في مفهوم أمن أنظمة الدفع تعيين موظفين مؤهلين ذو كفاءة للقيام بعمليات الدفع، ويتوجب على المشاركين في أنظمة الدفع وضع أنظمة نجدة أو ما يُطلق عليه باللغة الإنجليزية Back up، مع توفير الموارد البشرية الملائمة لغرض ضمان استمرارية الاستغلال الفعال لمواجهة كوارث كبيرة تُعرقل الاشتغال العادي للمنشآت الأساسية.

طبقا للمادة رقم: 11 من نفس النظام السالف الذكر، بنك الجزائر يتكفل بالسهر على السير الحسن لأنظمة الدفع ويسهر على أمن أنظمة المقاصة والتسوية، مع تسليم الوسائل المالية، أما المادة رقم: 12 من هذا النظام أوجبت كذلك مهمة بنك الجزائر في التأكد من أمن بطاقات الدفع الإلكترونية، ومتابعة إجراءات توفير كافة شروط الأمن التي قامت بها الجهات التي تصدرها "البنوك"، ومتابعة إحصاءات التدليس والتطورات المختلفة في ميادين التكنولوجيا التي قد تؤثر على أمن بطاقات الدفع الإلكترونية.[1]

2- الوسائل القانونية الدولية:

الأمن السيبراني هو مسألة عابرة للحدود بسبب الاستخدام الموسع للفضاء الإلكتروني في مختلف مجالات الحياة، ونظرا لكون الإنترنت شبكة دون سيطرة مركزية كون تملكها أو تديرها العديد من الكيانات المختلفة، أسهم هذا في بُروز مشاكل كبيرة على مستوى حماية الأنظمة والبيانات،[2] الأمر الذي يُحتم التعاون الدولي الذي ينبع من الطابع العالمي لشبكات الاتصالات، ويستدعي بذلك تشريعات وقوانين لحماية البيانات الشخصية على المستوى الدولي، والتي لها إطار عالمي تحت غطاء شرعية حقوق الإنسان والحريات الشخصية الصادرة عن الأمم المتحدة سنة 1948، التي أُقرت في المادة 12: "حق الشخص بعدم التعرض الاعتباطي لخصوصيته

[1] راجع المواد 5،6،11،12 من **نظام بنك الجزائر**، مرجع سابق، ص 24.

[2] يدري ربيعة، **نفس المرجع السابق**، ص465.

وحقه في حفظ كرامته وحقوقه الفردية"، ويندرج في هذا السياق الاهتمام في أنحاء العالم من خلال التعاون الدولي القضائي على المستوى الإجرائي الجنائي، وبين أجهزة الشرطة في الدول المختلفة عن طريق إنشاء مكاتب متخصصة مثل الإنتربول (INTERPOL)،* والأفريبول (AFRIPOL)،* والمركز العربي الإقليمي للأمن السيبراني (ARCC)،* من أجل التنسيق فيما بينها لضبط وتوقيف وتسليم المجرمين السيبرانيين الذين يتجاوزون حدود الدولة في جميع الجرائم والتي من بينها الجرائم الإلكترونية التي تمس بالمعلومات والبيانات الشخصية، بالإضافة إلى المساعدات المتبادلة لأغراض التحقيق وجمع القرائن الإلكترونية للعمل الإجرامي، تسليم المجرمين، الإنابات القضائية، ومن خلال ذلك أُبرمت العديد من الاتفاقيات الدولية والإقليمية متعددة الأطراف في مجال التعاون الدولي، ومن شأن هذا الإدماج أن يضاعف من الثقة،[1] وأن يكفل تطوير وتطبيق السياسات والتكنولوجيا بالشكل الملائم والأكثر فعالية في مكافحة الإجرام السيبراني.[2]

من بين هاته الاتفاقيات والمعاهدات على سبيل المثل لا الحصر:[3]

- اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة، سنة 2000.
- اتفاقية بودابست للتعاون الدولي لمكافحة الجرائم في مجال المعلومات الحاسوبية والاتصالات، سنة 2001.
- المعاهدة الدولية للمجلس الأوروبي لمكافحة جرائم الإنترنت، التي تضم 30 دولة، سنة 2010.
- المعاهدة الدولية للمجلس الأوروبي لمكافحة الجريمة السيبراني، سنة 2004.
- تشريعات الإسكوا في إطار مشروع تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية المنفذ خلال سنة 2012 "إرشادات الإسكوا للتشريعات السيبرانية".
- الاتفاقية العربية لجامعة الدول العربية بشأن مكافحة الجرائم التقنية للمعلومات، سنة 2010.
- اتفاقية مالابو للاتحاد الافريقي حول الأمن السيبراني وحماية البيانات الشخصية، سنة 2014.
- اتفاقية الامن السيبراني كبروتوكول إضافي لاتفاقية بودابست، سنة 2017.
- انشاء المكتب الاقليمي العربي للاتحاد الدولي للاتصالات لدراسة فعالية الامن السيبراني في المنطقة، سنة 2018.
- اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية التي صادقت عليها 65 دولة في مارس سنة 2020.

(*): **INTERPOL** منظمة بوليسية دولية أنشأت سنة 1923 تحت اسم اللجنة الدولية للبوليس الجنائي وتضم 194 دولة كأعضاء، مقرها الرئيسي بليون فرنسا.

(*): **AFRIPOL** منظمة الشرطة الجنائية الافريقية، أنشأت سنة 2015 في الجزائر، تضم 41 دولة كأعضاء، مقرها الرئيسي ببن عكنون الجزائر العاصمة.

(*): **ARCC** المركز العربي الإقليمي للأمن السيبراني، أنشأت سنة 2012، مقرها الرئيسي في سلطنة عمان.

[1] حنين جميل أو حسين، **الإطار القانوني لخدمات الأمن السيبراني، دراسة مقارنة**، رسالة ماجستير في القانون الخاص، كلية الحقوق، جامعة الشرق الأوسط، عمان الأردن، 2021، ص 59.

[2] مراد ماشوش، **الجرائم الاقتصادية وسبيل مكافحتها -الجهود الدولية لمكافحة الإجرام السيبراني**، دكتوراه في القانون العام الاقتصادي، كلية الحقوق والعلوم السياسية جامعة غرداية، الجزائر، سنة 2017/2016، ص 190.

[3] الموقع: Https://ar.wikipedia.org، تاريخ الاطلاع: 07-08-2023، على الساعة: 10:50.

وبالرغم من كل المجهودات المبذولة من طرف الدولة، يرى أهل الاختصاص أن البُنية التنظيمية والتشريعية مازالت في طور التشكيل حتى تكتمل المعادلة، على اعتبار أن القوانين التي تحوي قواعد مُلزمة ورادعة أخذت حصة الأسد في التشريع، في حين أن هناك العديد من الجوانب لم يتم تطويرها بما يتوافق مع البيئة الدولية، كالمقاييس والمعايير الدولية للحماية والأمن، المواصفات التقنية للمعلومات والبيانات، الأنظمة، البرامج والأجهزة الحديثة.[1]

المطلب الرابع: الوسائل البشرية لحماية البيانات في الفضاء السيبراني (Human Means)

إن دور التقنية يقتصر على توفير الأجهزة وملحقاتها فقط، لكن يلعب العنصر البشري دورا كبيرا وأساسيا في توجيه وتطويع هاته الأجهزة التقنية والبرامج المساندة لها، إذ هو المكون الجوهري الذي يجب أن تُبنى عليه السياسات التي ستعمل على تنفيذ برامج الأمن السيبراني، كما أجمعت العديد من الأبحاث والدراسات والتقارير الدولية على أن العنصر البشري يُسهم بأكثر من 90% في برامج الأمن السيبراني وذلك من خلال: (بحوث ودراسات أكاديمية، تطوير أجهزة تقنية، تطوير برمجيات، ثقافة وتوعية مجتمعية، برامج تكوين وتدريب، سياسات إعلامية، قوانين وتنظيمات، اتفاقيات ومعاهدات دولية،...إلخ)، فكل هذه العناصر هي تعتمد على الكفاءات والقدرات البشرية بشكل خاص.

مفهوم الكفاءات البشرية يُعتبر من أهم المفاهيم التي تستدعي انتباه المسيرين والمنظرين، ذلك لأن تلك الكفاءات هي المصدر الرئيسي للميزة التنافسية المستدامة، خاصة لدى المؤسسات المالية كالبنوك التي أصبحت تلعب دورا هاما ومحوريا في اقتصاديات الدول، ما يتطلب تطوير وتنمية المورد البشري للارتقاء بجودة الخدمات الإلكترونية المقدمة ورفع مستواها، علما أن المصارف الناجحة هي المصارف التي استطاعت أن تقضي على الثغرات الأمنية والنواقص في كفاءة كوادرها، ومدى استعداد تلك الكوادر للتعامل مع الوسائل التكنولوجية المتطورة وأمنها السيبراني كونها أضحت محفوفة بالمخاطر والتهديدات.

كما لا يستقيم تعريف الكفاءة إلا في ظل تكامل عدة مكونات كالمعرفة، المهارة، القيم، السمات، الدوافع، المفهوم الذاتي، حيث تتكامل مع بعضها البعض دون عزل مكون عن الآخر.[2]

ويُعد العنصر البشري من الركائز الأساسية للارتقاء بالأداء المصرفي، على اعتبار أن الكفاءة في الأداء هي الفاصل ما بين المصارف، فمهما تنوعت مصادر الكفاءة يظلُ العامل البشري وراءها، من أجل مسايرة أحدث ما وصل إليه العلم في مجال التكنولوجيا المصرفية، لذا ينبغي تطوير إمكانيات العاملين وقدراتهم لاستيعاب التطورات في مجال الخدمات الإلكترونية المصرفية وأمنها السيبراني، بما يُحقق تحسين تقديمها بكفاءة وتحقيق أفضل

[1] جمال بوزادية، **نفس المرجع السابق**، ص 1278.

[2] حمدي أبو القاسم الأخضر، **دور التعلم غير الرسمي في تنمية كفاءات الموارد البشرية**، مجلة دراسات، جامعة الأغواط، العدد 43، جوان 2016، ص 250.

استخدام للموارد البشرية في المصارف الجزائرية، إذ يتطلب الارتقاء بالعنصر البشري تبني العديد من الاستراتيجيات نذكر منها:

- الاستعانة بذوي الخبرة ومكاتب الاستشارة الدولية في تدريب الكوادر المصرفية على استخدام أحدث النظم التقنية المصرفية.
- وضع نموذج لتقييم أداء العنصر البشري من خلال عدة معايير تأخذ في اعتبارها أداء الوحدة ودوره في تحقيق أفضل النتائج.
- الرفع من مستوى كفاءة العاملين بإعطاء الأولوية في التوظيف لخريجي الجامعات وذوي المهارات.
- إنشاء معاهد متخصصة وتطوير البحث العلمي في ميدان الخدمة الإلكترونية المصرفية وأمنها السيبراني.
- التكوين المتخصص في مختلف مجال الأمن السيبراني، الشبكات ونظم المعلومات، الإعلام الآلي، هندسة الأنظمة، الإعلام الآلي، الذكاء الاصطناعي والوسائط المتعددة، هندسة البرمجيات، خوارزميات البرمجة...الخ

من الناحية العملية في استغلال العنصر البشري قصد ضمان التنفيذ الفعلي لمختلف التدابير وإجراءات الأمن السيبراني في الجزائر أُوكلت مهام تطبيق القانون وردع الجريمة السيبرانية إلى هيئات متخصصة ضمن أسلاك الأمن المختلفة، هاته الهيئات هي كما يلي:[1]

- المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة للمديرية العامة للأمن الوطني.
- مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها للدرك الوطني.
- المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني.
- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة لدائرة الاستعمال بالجيش الوطني الشعبي.

المطلب الخامس: المواصفة القياسية الدولية ISO 27032 لإدارة أنظمة الأمن السيبراني وآليات تعزيزه في المصارف الإلكترونية

تُعد حماية البنية التحتية الحيوية للمصارف الإلكترونية من المهام الرئيسية للأمن السيبراني من شتى أنوع الحوادث والمخاطر السيبرانية، وهذا من خلال تعزيز سلامة البنية التحتية للمعطيات التي تعتمد عليها مختلف القطاعات وتأمين الشبكات والخدمات الموفرة للاحتياجات اليومية للمستعملين، فالخطر السيبراني وتهديداته هي في تصاعد يُقابله انتشار الأدوات والمنهجيات على أوسع نطاق بتطور تقنية المجرمين السيبرانيين،[2] ما

[1] جمال بوزادية، "**نفس المرجع السابق**، ص 1279.

[2] أبو الحسن حنين جميل، **الإطار القانوني لخدمات الأمن السيبراني – دراسة مقارنة**، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، 2021، ص49.

يستوجب تعزيز آليات مختلفة لضمان أمن البيانات والمعلومات في القطاع المصرفي، ومن بين هاته الآليات ما يلي:

1- ضرورة الاعتماد على معايير الحماية الدولية الرسمية ISO 27032 لإدارة أنظمة الأمن السيبراني:

ISO 27032: عبارة عن معيار عالمي يعنى بحماية المعلومة، له متطلبات معينة عند تلبيتها تحصل المنظمة على شهادة معتمدة تفيد بتطبيقها للمعايير الواردة على نطاق العمل الذي تم اختياره بمعنى أنه أولا يتم تقييم مدى التوافق مع المعايير (ويحصل هذا دوريا مرتين خلال العام) وبعد اجتيازه التقييم تحصل المنظمة على شهادة معتمدة بموافقتها للمعيار 27032، حيث يعد معيار الحماية الدولي الرسمي المقدم لأي منظمة (بغض النظر عن كونها صناعية كانت أم خدمية) ترغب بالحصول على شهادة مستقلة لنظام إدارة حماية المعلومات الخاصة بها وتحسين وضع الأمن السيبراني في المنظمة من خلال وضع إطار للأمن مبني على إدارة المخاطر، لهذا تحدد المواصفة المتطلبات الإلزامية لتأسيس وتطبيق وتوثيق النظام وتحديد متطلبات السيطرة لحماية المعلومات التي ستطبق وفق حاجات المنظمة الخاصة بها، وتشمل 14 مركز خاص بالسيطرة و39 هدف، حيث يرتكز على مفاهيم السرية، السلامة، والتوافر، التحقق من الهوية، متابعة الطلب وإمكانية التعقب، المرجعية، عدم التخلي، والعديد من الميكانيزمات الأخرى،[1] ومن أهم الفوائد المتحققة من جراء استخدام المواصفة القياسية ISO 27032 تحقيق نوع من الثقة بين المنظمات والعملاء والموردين والشركاء، تحسين فعالية الحفاظ على الأمن السيبراني للبيانات، الشرعية، تحقيق سلامة وجودة السلع والخدمات، تشكيل نظام تكامل يجمع أحاب المصلحة في الفضاء السيبراني.[2]

2- الحصول على أحدث التقنيات: وهذا فيما يتعلق بالبرامج (Software)، والأجهزة (Hardware)، لمواجهة آخر التطورات والأساليب المتبعة في مجال الهجمات والقرصنة الإلكترونية الدولية، بهدف اقتناء جدار أمني أكثر فعالية قادر على التصدي لأحدث الأساليب المتبعة في هذا الشأن.

3- تخصيص الموارد المالية: يجب أن تكون الموارد المالية كافية للحصول على أحدث التقنيات في مجال الأمن السيبراني، مع العلم أنها تتسم بالارتفاع في تكلفة اقتناءها.

4- تنظيم ندوات وورشات عمل وتوفير دورات عالية المستوى ومؤتمرات: يكون ذلك بمشاركة الشركات والمؤسسات الدولية المتطورة في مجال التقنيات لاطلاع الكوادر الفنية على أحدثها قصد مواكبة التطور السريع والتعرف على مختلف التقنيات في مجال أمن الخدمات الإلكترونية المصرفية على المستوى العالمي، وهذا بهدف خلق كوادر فنية عالية المستوى قادرة على التصدي للتحديات الجديدة المرتبطة بهذه التقنيات والتغلب عليها.

---

[1] Fernandez Toro, Sécurité Opérationnelle, **"conseil pratique pour sécuriser le système d'information"**, Eyrolles, 2016, P 23.

[2] الموقع: https://www.rmg-sa.com، تاريخ الاطلاع: 23-09-2023، على الساعة: 22:00.

5- قيام الهيئات والجهات الرقابية في الدولة بإصدار تعليمات وقواعد منظمة: في مجال المصارف والمؤسسات المالية يكون بإجراء عقود لأطراف ثالثة تختص بأمن نظم المعلومات والأمن السيبراني، على أن تخضع تلك الشركات التي يتم التعهيد إليها للرقابة الصارمة من قبل الأجهزة الأمنية، بهدف القضاء على عمليات القرصنة والاحتيال على الأنظمة الإلكترونية.

6- القيام بتوعية المستخدمين: من خلال البرامج المسموعة والمرئية والندوات التثقيفية تتم التوعية لرفع مستوى ثقافة الأمن السيبراني، بهدف تفهم الضوابط والتعليمات الخاصة بأمن نظم المعلومات المصرفية.

7- إلزام السلطات للمصارف بتضمين استراتيجيات المخاطر: العمل على تضمين الاستراتيجيات المقرَة من قبل مجالس إدارات المصارف أو المصرف المركزي مع ضرورة تنفيذها، بهدف وضوح السياسة الأمنية السيبرانية للبنك.

8- إلزامية وجود إطار عمل لإدارة المخاطر وضمان الجودة: يكون هذا في تقديم الخدمات الإلكترونية المصرفية المختلفة مع القيام بدوريات تقييم المخاطر.

9- تنظيم وإدارة الحسابات والخدمات المصرفية المقدمة عبر الإنترنت: حيث تتمثل مسؤولية المصرف في اتخاذ الاعتبارات اللازمة نحو الحفاظ على سرية البيانات وخصوصيتها التي تحقق هوية العميل عند الاستفادة من تلك الخدمات الإلكترونية، بتطبيق أساليب فعَالة يمكن الاعتماد عليها للتحقق من هويته وصلاحية دخوله.

10- مراعاة المصرف التدابير الرقابية عند التعامل مع كلمة السر الخاصة بالعملاء: بحيث يتم تطبيق الرقابة المزدوجة من خلال الفصل بين عملية إنشاء كلمات السر وتسليمها للعملاء، وعملية تفعيل حسابات الخدمات الإلكترونية المصرفية، مع تعزيز تأمين عملية إنشاء كلمات السَر لضمان عدم تعرضها للاطلاع أو كشف، كما يجب التأكد من أن كلمات السر لا يتم ارسالها أو تخزينها أو معالجتها كنص واضح.

11- تطبيق مبدأ الرقابة المزدوجة: وهذا على مختلف تحويلات أموال العملاء إلى مستفيدين آخرين، مع إلزام المصرف بوضع حد أقصى يومي لعمليات التحويل.

12- إجراء اختبارات أمنية: تكون بصفة دورية على مختلف التطبيقات المصرفية قبل تثبيتها وبعده، مع اتباع نهج استباقي للكشف عن الثغرات الأمنية والمعاملات الاحتيالية المحتملة.

13- قيام البنك بتقييم نقاط الضعف: تلك الموجودة في النظم والتطبيقات مرتين على الأقل سنويا، ووضع خطة للحد منها قصد تقليل المخاطر.

14- فرض المصرف المركزي على المصارف الأخرى القيام بعملية اختبارات الضغط " Stress Testing": لتحديد حجم الآثار المترتبة على نجاح أية عمليات قرصنة تتعرض لها الأنظمة الإلكترونية المصرفية، بصفة دورية سنوية أو نصف سنوية.

15- إبلاغ السلطات المختصة عن الاختراقات وأية عمليات إجرامية إلكترونية ساعة وقوعها: لتقفي الأثر وضبط الدليل وتحديد هوية الفاعل.

16- تدريب وتكوين القدرات البشرية في القطاع المصرفي في مجال أمن الفضاء السيبراني: من خلال دعم التعليم الأكاديمي المتخصص والبعثات الدراسية الخارجية، مع الأخذ بالاعتبار المقترحات والمبادئ الرقابية الصادرة عن المؤسسات والهيئات الدولية المختصة في هذا الشأن.[1]

[1] مروة فتحي السيد البغدادي، **نفس المرجع السابق**، ص ص 1491-1498.

خلاصة الفصل الأول:

في هذا الفصل تناولنا الأدبيات النظرية التي تشكل الإطار المفاهيمي للأمن السيبراني للبيانات، وهذا قصد تنوير موضوع البحث والتمهيد للإجابة عن إشكالية الدراسة المطروحة، حيث في المبحث الأول قمنا بتعريف الأمن السيبراني والتطرق إلى الفرق بينه وبين مصطلحي الأمن المعلوماتي والأمن الإلكتروني، وذكر أهداف الأمن السيبراني وخصائصه ومستوياته وأبعاده، لننتقل للحديث في المبحث الثاني عن مفهوم البيانات الشخصية من خلال التعاريف المختلفة المقدمة لها، وتبيان العلاقة بين البيانات والمعلومات والفرق بينهما، ثم التطرق إلى الرقابة على أمن بيانات العملاء في المصارف الإلكترونية وكذا الحديث عن آلية التخزين السحابي لهاته البيانات في البنوك الإلكترونية، وفي الجانب الآخر من المخاطر قمنا بالتنويه لأنواع التهديدات السيبرانية الماسة بأمن البيانات، أما في المبحث الثالث المتعلق بإستراتيجية الأمن السيبراني ووسائل حماية البيانات من مخاطر الفضاء السيبراني، قمنا بتعريف محاور إستراتيجية الأمن السيبراني، ثم شرح وسائل حماية البيانات انطلاقا من الوسائل التقنية، إلى الوسائل القانونية والتشريعية، وصولا إلى الوسائل البشرية والكفاءات، وفي النهاية عرضنا المواصفة القياسية الدولية ISO 27032 لإدارة أنظمة الأمن السيبراني وآليات تعزيزه في المصارف الإلكترونية، وقلنا أن هاته الأخيرة من أجل تحقيق أهدافها والوصول لغاياتها هي مطالبة بأن تزيد من إجراءات أمنها السيبراني ودفاعاتها الإلكترونية حتى تعزز من ثقة عملائها.

الفصل الثاني

الثقة في الخدمات الإلكترونية المصرفية

تمهيد:

إن النمو السريع في استخدام التكنولوجيا الحديثة وشبكة الإنترنت يحمل العديد من الفرص والمزايا التنافسية لكافة منظمات الأعمال بصفة عامة وللبنوك بصفة خاصة، فالعمليات المختلفة عبر الإنترنت والعلاقات المتبادلة بين الأطراف تتطلب وجود عامل الثقة، كما أشار كونولي Connolly إلى أن ثقة العميل أصبحت أكثر أهمية من أي وقت مضى، حيث لم تعد الوسائل التقليدية في السابق لبناء الثقة والحفاظ عليها فعّالة بسبب العدد الهائل لمنصات الخدمات الإلكترونية المصرفية والوضع التنافسي لها، لذلك أصبح لزاما على الشركات والمؤسسات البحث عن طرق جديدة لبناء ثقة العميل في الخدمات الإلكترونية المصرفية، ومن جهة أخرى أُشير في عدة بحوث ودراسات أن استخدام الخدمات الإلكترونية المصرفية يُؤثر تأثيرا كبيرا على ثقة العملاء في المصارف الإلكترونية بسبب عدم توافر عنصر الأمان، ومن هذا المنطلق، سنتناول في فصلنا هذا مختلف الأدبيات النظرية التي لها صلة بموضوع الثقة في الخدمات الإلكترونية المصرفية، عليه تم تقسيم الفصل إلى ثلاثة مباحث كما يلي:

- المبحث الأول: ثقة العملاء.
- المبحث الثاني: الخدمات الإلكترونية المصرفية.
- المبحث الثالث: ثقة العملاء في الخدمات الإلكترونية المصرفية.

المبحث الأول: ثقة العملاء (Customer Trust)

تُعتبر الثقة عامل مهم من عوامل نجاح المؤسسة المصرفية التي تقدم خدماتها إلكترونيا، إذا أحسنت استغلالها أصبحت جزءً لا يتجزأ من ميزتها التنافسية، في ظل بيئة إلكترونية هي في أعز حاجة إلى إرساء قواعد ومبادئ الثقة الرقمية، خاصة إذا ما علمنا أن جميع الخدمات المقدمة من قبل أي مؤسسة رقمية هي محفوفة بالمخاطر، والمؤسسة المصرفية هي أولى هاته المؤسسات كون نشاطها يتعلق بالمال الذي لا يقبل صاحبه المخاطرة.

المطلب الأول: تعريف الثقة (Confidence)

* **المعنى اللغوي**: ورد مصطلح الثقة في المعاجم العربية تحت كلمة (وثق به، يثقُ بك ثقةً إذا اتمنك).

* **المعنى الاصطلاحي**: وهي ذلك الشعور الإيجابي الذي يملكه الفرد تجاه الطرف الآخر من حيث ثقته بقيامه بالأعمال والأفعال المتفق عليها.

وتُعرَف الثقة بشكل عام بأنها: "احتمال ذاتي بأن يتوقع أحد الفاعلين أن يقوم فاعل آخر بعمل معين تعتمد عليه فائدته"، كما عرفها أيضا: McKningt وChervany بأنها: "رغبة شخص في الاعتماد على شخص آخر في سياق مُعين يشعر فيه بالأمان حتى لو صاحب ذلك حدوث عواقب سلبية".[1]

إذا فالثقة تقوم على شخصين أحدهما هو المبادر بالثقة، والآخر هو الذي تُوضع فيه هذه الثقة، وذلك في سياق علاقات ومعاملات متنوعة.

كما فسَرها بعض الباحثين في مجال تسويق الخدمات على أنها: "درجة إيمان وتقبل الفرد للقرارات والسياسات التي تضعها إدارة المنظمة، والتي تقوم بتنفيذها وإدارتها بشكل عادل لجميع الأطراف"،[2] وهي أكثر أهمية في المجال الخدمي والمسوقين.[3]

ولتوضيح أكثر لمفهوم "الثقة"، قمنا بعرض مجموعة من المفاهيم التي تطرق إليه بعض باحثي التسويق، كما هو موضح في الجدول الموالي رقم (II-1):

---

[1] خادم نبيل، **دور بناء الثقة في تطوير المعاملات الرقمية**، فرنسا أنموذجا، مجلة الفكر القانوني والسياسي، المجلد 05، العدد 01، 2021، ص 143.

[2] Héla Chérif Benmiled, **La confiance en Marketing**, Recherche et Application en Marketing, Vol 17, N 4, Université Paris, France, 2012, PP 141-155.

[3] Devon Johnson and Kent Grayson, **Sources and Dimensions of Trust in Service Relationships**, **in T.A Lacobucc**, **Hanbook of Services Marketing and Management**, New yourk: SAGE Publication, Inc, 2000, P 357. sttps://doi.org/104135/9781452231327.n24, Retrieved: 01-04-2022, 21:10.

جدول رقم (II–1): مفاهيم " الثقة " من منظور بعض باحثي التسويق

اسم الباحث	مفهوم الثقة
Morgan Robert and Hunt Shelby (1994)	الثقة هي قناعة الزبون باستقامة البائع الذي يتعامل معه وإمكانية الاعتماد عليه، حيث تحدُث الثقة عند امتلاك طرف ما ثقة (Confidence) في أمانة وصدق شريك التبادل.[1]
Gefen David (2000)	الثقة في التاجر على الإنترنت، هي رغبة أحد الأطراف لجعل نفسه عرضة لأعمال الطرف الموثوق فيه وفقا للشعور بالأمان والضمان والموثوقية.[2]
Sulin Ba and Pavlou Paul (2002)	الثقة هي التقييم الشخصي لأحد الأطراف بأن الطرف الآخر سيؤدي عملية معينة وفقا لتوقعه في بيئة تتسم بعدم التأكد.[3]
Salo Jari and Karjaluoto Heikki (2007)	الثقة هي الرغبة للاعتماد على أمانة وقدرة وخصائص الشخص الموثوق فيه وقراره، حتى ولو كانت النتيجة غير معروفة حاليا.[4]
Roy Sanjit (2011)	الثقة تعتبر عنصرا مهما يركز على العلاقات بين البائع والمشتري.[5]
Rotter Julian (1967)	الثقة هي توقع الفرد على أنه يمكن الاعتماد على الكلمة أو الوعد أو الكلام الشفهي أو الكتابي لفرد آخر.[6]
Sidersmukh and al (2002)	الثقة هي توقعات الزبائن بأن مقدم الخدمة يمكن الاعتماد عليه في الوفاء بالوعود المقدمة من طرفه.[7]

1 Morgan Robert and Hunt Shelby, **The Commitment Trust Theory of Relationship Marketing**, Journal of Marketing, Published By: Sage Publication, INC, Vol 58, N 3, 2015, P 20-38. https://doi.org/10.2307/1252308

2 Gefen David, **E-Commerce**: **The Rol of Familiarity and Trust OMEGA**, Vol 28, N 6, 2000, P 725-737. https://doi:10.1016/S0305-0483(00)00021-9.

3 Ba Sulin, Pavlou Paul, **Evidence of Trust Building Technology in Electronic Markets**: **Price Premiums and Buyer Bahavoir**. **MIS Quality**, Vol 26, N 03, 2002, P 243-268. https://doi.org/10.2307/4132332.

4 Salo Jari, Karjaluoto Heikki, **a Conceptual Model of Trust in the Online Environment**, **Online Information Review**, Vol 31, N 5, 2007, P 605. www.emeraldinsigh.com/1468-4527.htm.

5 Roy Sanjit, **Dimensions of True and Trustworthiness in Retail Banking**: **Evidence from India**, Marketing Management Journal, Vol 21, N 1, 2011, P 98.

6 Rotter Julian, **A New Scale For the Measurement of Interpersonal Trust**, Journal of Personality, Vol 35, N 4, December 1967, P 651-665. https://doi.org/10.1111/j.1467-494.1967.tb01454.x.

7 Deepak Sideshmukh, Jagdip Singh, Barry Sabol, **Consumer Trust**, **Value**, **and Loyalty in Relational Exchanges**, Journal of Marketing, Vol 66, N 1, 2002, P 15-37.

Mircea Fuciu 2017	الثقة تُمثل مقياسا احصائيا لمشاعر العملاء حول الحاضر والمستقبل للظروف الاقتصادية، وتُستخدم كمؤشر للحالة العامة للاقتصاد.[1]

المصدر: من اعداد الطالب بالاعتماد على المراجع.

❖ **يمكن أن نستنتج من خلال التعاريف السابقة أن: "الثقة هي توقعات طرف معين مع إرادته الفعلية للاعتماد على طرف آخر دون غيره في تحقيق نتائج مرغوبة، مع استعداده لقبول درجة الخطر".**

المطلب الثاني: الثقة العادية والثقة الرقمية

هناك من يرى أن الثقة تُعتبر مُكافئًا وظيفيا للمعرفة بنوايا الطرف الآخر، لهذا يرى عالم الاجتماع جيدنز أنتوني Anthony Giddens أن: "الموقف الأول الذي يتطلب الثقة ليس غياب القوة، بل غياب المعلومات الكافية"،[2] وهو ما يبدو جليا في المعاملات الإلكترونية التي تنحصر فيها العلاقة المادية بين الأطراف، إذ أنها لا تشترط حضورهما في نفس المكان (عالم الافتراض)، وهذا ما يُؤدي إلى نقص المعلومات حول الطرف الآخر.

إذا يمكن تعريفها في هذا الإطار بأنها: "علاقة بين كيانين تقوم على اعتقاد شخصي للكيان الأول (صاحب الثقة) "Trusting Party" بقدرة الثاني (الموثوق فيه)" Trustee" على أداء خدمة مُعينة بطريقة متوقعة ومهنية، والامتناع عن أي سلوك خبيث أو غير مُتوقع أثناء القيام بهذه الخدمة"،[3] وتعرف أيضا بأنها: "اعتقاد ذاتي من المؤتمن في جهات تُقدم خدمات إلكترونية، ويتميز بكونه قابلا للقياس بتوظيف جميع مصادر المعلومات المتاحة والمتعلقة بالجهة التي تقدم الخدمات، وتشمل: الخبرة، السمعة، الجودة، المخاطر....الخ"،[4] وهناك من يجعل منها ضرورة للتغلب على أوجه عدم اليقين المتصورة في المعاملة الرقمية، والتي تهدف للوثوق بالطرف الآخر بأنه أهل للقيام بخدمة رقمية تتسم بالنزاهة والمصداقية.[5]

---

[1] Mircea Fuciu, **The Consumer Confidence Report– A Tool For Developing Marketing Strategies Designed For The Online Environment**, Annals Univeresitatis Apulensis Series Oeconomica, Vol 19, N 2, 2017, P 30-38. https://doi:10.29302/oeconomica.2017.19.2.3.

[2] حادم نبيل، **المرجع السابق ذكره**، ص 143.

[3] Ait Mouhoub Younes et Bouchebbah Fatah, **Proposition d'un modèle de confiance pour l'Internet des Objets**, Mémoire de master, Université A/Mira de Bejaia, Faculté des Sciences Exactes, Promotion 2015, p10.

[4] Van-Hoan Vu, **Infrastructure de gestion de la confiance sur internet**, thèse de doctorat, Ecole Nationale Supérieure des Mines de Saint-Etienne, Français, 2010, p 21.

[5] Ayten Okusz and all, **Trust in the Information Systems Discipline in Trust and Communication in a Digitized World**: **Models and Concepts of Trust Research**, Springer International Publishing Switzerland, 2016, p 209.

من هنا فإن "**الثقة الرقمية**": هي واحدة من عوامل نجاح المصارف التي تقدم خدمات إلكترونية وتُعزز قدرتها على تأدية رسالتها ورُؤيتها، كما أشار كليمان (Climan) أن الثقة الرقمية: "هي تعني أن تقوم المؤسسة على توفير المتطلبات العصرية والرقمية والاتصالية، وتضمن الاستخدام الآمن لها، وأن المستخدم يمكنه الاعتماد على البيانات والمعلومات، وأن ما يحصل عليه هو آمن وصادق".[1]

وأشير إلى أن: "الثقة الرقمية من متطلبات إرساء مجتمع المعرفة، وإدارة المعرفة، وأنها أصبحت جزءً من الميزة التنافسية لكثير من المؤسسات، وفي ظل بيئة تعلم إلكترونية فإن هناك حاجة لإرساء قواعد ومبادئ الثقة الرقمية، وأن يكون هناك نماذج وبرامج حماية تُسهم في تعزيز ثقة المستخدم بالبرامج والتقنيات، وأن يُدرك المستخدم أنه في مكان رقمي آمن".[2]

وفي بحثنا هذا نحن نبحث عن مفهوم الثقة الرقمية في مجال الخدمات الإلكترونية المصرفية، أين قُدمت العديد من الدراسات لباحثي التسويق، فكانت كما يلي:

ينظر كل من Ennew and Sekhon للثقة الرقمية في المجال المالي على أنها: "استعداد الفرد لقبول الضعف على أساس التوقعات الإيجابية حول نوايا أو سلوك شخص آخر في موقف يتسم بالاعتماد المتبادل والمخاطر"،[3] أما Jarvinen Raija فيرى ثقة العملاء في البنوك أنها: "تستند على تجربة العميل وتعتمد على قدرة البنك على التصرف بطريقة موثوقة ومراعاة القواعد واللوائح التنظيمية، والعمل بشكل جيد وخدمة المصلحة العامة ووفاء البنك بوعوده"،[4] ويرى Peng Lee, Moghavemi أن الثقة في القطاع البنكي تعني أن البنك جدير بالثقة والصدق والنزاهة، وموثوق به في تقديم الخدمات لزبائنه.[5]

حيث هناك ثلاثة اعتبارات أساسية لثقة العميل في بيئة الأعمال الإلكترونية المصرفية تتمثل في:

1-الثقة في الإنترنت: إن الثقة في الأعمال الإلكترونية هي تشمل فكرة الثقة في البنية الأساسية وآلية التحكم المستخدمة (ثقة التكنولوجيا)، والتي تتعامل بأمانة وسرية ومصداقية العمليات، فالثقة البشرية في أي نظام إلكتروني

---

[1] كليمان سارة غران، **التعلم الرقمي: التربية والمهارات في العصر الرقمي**، الندوة الاستشارية المعنية بالتعلم الرقمي التي عقدت كجزء من برنامج معهد كورشام للقيادة الفكرية: (Corsham Institute Thought Leadership Programme)، 2018، ص 47.

[2] نذير غانم، معمر جميلة، ريحان عبد الحميد، عنكوش نبيل، **الثقة الرقمية ضمن إستراتيجية الجزائر الإلكترونية 2013 واقعها ودورها في إرساء مجتمع المعرفة**، أعمال المؤتمر الثالث والعشرون: الحكومة والمجتمع والتكامل في بناء المجتمعات المعرفية العربية، ج 1، الدوحة، قطر، 2012، ص 76.

[3] Ennew Christine and Sekhon Harjit Singh, **Measuring Trust in Financial Services**: **The Trust Index**, Vol 17, N 2, 2007, P 62-68. Publication at: https://www.researchgate.net/publication/285769675.

[4] Jarvinen Raija, **Consumer Trust in Banking Relationships in Europe**, International Journal of Bank Marketing, Vol 32, N 6, 2014, p 554.

[5] Peng Lee, Moghavemi, **The Dimension of Service Quality and Its Impact on Customer Satisfaction, Trust, and Loyalty**: **A Case of Malaysian Bank**, Asian Journal of Business and Accounying, Vol 8, N 2, 2015, p 98.

أو آلي تعتمد على ثلاثة عوامل مهمة هي: الكفاءة الفنية المدركة للنظام، ومستوى الأداء المدرك للنظام، وفهم المشغل البشري للخصاص والعمليات التي تحكم سلوك النظام.

2-الثقة في مقدمي الخدمات عبر الإنترنت: قد أوضحت العديد من الدراسات أن المعتقدات المرتبطة بالثقة هي ذات تأثير قوي على نوايا العملاء لاستخدام الخدمات الإلكترونية، كما أن نقص الثقة هو مُبرر أساسي لعدم استخدامها، فالقرارات المتعلقة بالجدارة بالثقة للبائع الإلكتروني حتما تكون نتيجة للعمليات المتراكمة في الماضي (الثقة المعرفية) ونتيجة لأسس عاطفية (الثقة العاطفية).

3-الثقة في الطرف الثالث: تتمثل ثقة الطرف الثالث في مجال التعامل الإلكتروني أو الشراء عبر الإنترنت في الثقة في المؤسسات وضامني الطرف الثالث الذين يقومون بالتعامل بالفعل والالتزام والقدرة والنفع والتعهد بالأمانة...الخ، وهذا النوع من الثقة يكون على الأرجح لحل المخاوف المرتبطة باحترام الخصوصية.

الثقة الرقمية مفهوم ديناميكي مُتغير يشتمل على مرحلتين مختلفتين، المرحلة الأولى هي الثقة قبل توظيف التكنولوجيا "ثقة ما قبل الاستخدام"، والمرحلة الثانية هي الثقة بعد توظيف التكنولوجيا "ثقة ما بعد الاستخدام"، فكلا النوعين يعدل من سلوك المستخدم للتكنولوجيا، وللتوضيح أكثر ففي حالة ثقة ما قبل الاستخدام تؤثر الثقة على نوايا المستخدم نحو تبني التكنولوجيا وقبولها، بينما تقوم ثقة ما بعد الاستخدام بتعديل نوايا المستخدم للاستمرار في استخدام التكنولوجيا، وعلى الرغم من هذا الفرق الواضح بين ثقة ما قبل الاستخدام وثقة ما بعد الاستخدام فإن القليل من الدراسات وصفت بشكل واضح المرحلة التي يتم فيها فحص الثقة.[1]

كما تختلف الثقة الرقمية (Online Trust) عن الثقة العادية (Offline Trust) بالنسبة للخدمات المصرفية الإلكترونية، في العديد من الجوانب نذكر أهمها:

-أن الثقة الرقمية نتيجة تفاعلات الأفراد مع نظام المعلومات الإلكتروني عبر الإنترنت.

-الانفصال أو وجود مسافة طبيعية مادية بين طرفي التعامل (العميل-المؤسسة المصرفية).

-غياب رجال البيع والانفصال بين الخدمة والعميل.

-غياب الاهتمام بالمكان والوقت المستغرق من جانب العميل.

-غياب الخصائص البشرية للشبكة الإلكترونية والتغذية العكسية والقدرة على التعلم، والتعامل المتواصل الذي لا وقت له.

كما تختلف علاقات الثقة الرقمية عن تلك العلاقات المرتبطة بالثقة العادية، فقد تناول علماء النفس وعلماء الاجتماع أشكالا عديدة من العلاقات بين أطراف الثقة (Trustor/Trustee) كما تحدث في بيئة الأعمال العادية غير الإلكترونية، حيث تكون أطراف الثقة فيها: أفراد، أو مجموعات والمجموعات قد تكون عائلات،

[1] Hernandez José Mauro, Mazzon José Afonso, **Adoption of Internet Banking: Proposition and Implementation of an Integrated Methodology Approach**, International Journal of Bank Marketing, Vol 25, N 2, 2007, PP 72-88.

جيران، أو منظمات، أو مجتمعات، بينما في بيئة الأعمال الإلكترونية، فهناك مدخلان لتحديد العلاقات بين أطراف الثقة والأشياء محل الثقة (Objects of Trust)، الأول بحث الاتصالات المتوسطة بالكمبيوتر والذي قام الباحثون فيه بدراسة علاقات الثقة بين فرد وآخر، أو مجموعة أفراد تتوسطها التكنولوجيا، بينما على النقيض أو الوجه الآخر نجد بعض الباحثين ركز على التكنولوجيا كطرف (as Object) في الثقة أو العلاقة، كما أوضح Shankar سنة 2002، أن الثقة الرقمية تختلف عن الثقة العادية في أطراف الثقة، ففي الثقة العادية تكون أطراف الثقة شخص أو منظمة، بينما في المجال الرقمي تكون التكنولوجيا المتمثلة في الإنترنت أحد أطراف هذه الثقة، ومن وجهة النظر التسويقية تكون أطراف الثقة البائعين أو مقدمي الخدمات أي الشركات الممثلة لهم، فالعملاء في التجارة الإلكترونية لا يثقون في الموقع الإلكتروني (Website)، بل أيضا لا يثقون في الشركة التي وراء هذا الموقع، وهذا يوضح الطبيعة المعقدة الصعبة للثقة في التبادلات التجارية الإلكترونية.

والجدير بالذكر، أن العديد من نتائج الثقة العادية يمكن أن تطبق على البيئة الرقمية، فكل من الموافق، والظروف العادية، والرقمية، هي تشترك في وجود عملية التبادل بين المتعاملين، كما أن الخطر، والخوف، والتعقيد، والتكاليف وغيرها، هي من القيُود التي تُعيق أو تُقيَد عملية التبادل، وأن التعاون والتنسيق يزيد ويُحسن ذلك.

علاوة على ذلك، فإن القواعد الاجتماعية للتفاعل بين الناس تظهر كدالة في كل من البيئتين الرقمية والعادية، كما أنه توجد صلة قوية بين بحوث الثقة العادية والثقة الرقمية، فالقيام بإجراء البحث في الأخيرة يعتمد على العديد من بحوث الثقة العادية غير الرقمية، فمنذ عمل الثقة على الحد من الخطر، والخوف، والتعقيد في البيئة العادية، فهي تبدو أنها تفعل نفس الأشياء في البيئة الرقمية، فالثقة كرأس مال اجتماعي هي تخلُق التعاون والتنسيق في بيئة الأعمال العادية، ومن المتوقع أن يُفعل ذلك أيضا في البيئة الرقمية.[1]

المطلب الثالث: خصائص الثقة وأهميتها في البنوك الإلكترونية

إن للثقة أهمية كبيرة وعدة خصائص تسهم في كسب ود العملاء وتجذبهم من أجل استخدام الخدمات الإلكترونية المصرفية، عليه نتطرق إلى خصائصها كالآتي:

❖ خصائص الثقة:

تتميز الثقة بمجموعة من الخصائص نذكر منها:

-الثقة معيار شخصي ذاتي، وبناءً على ذلك فإن لكل شخص إدراك مختلف للثقة عن إدراك شخص آخر بالرغم من نفس الظرف أو نفس الموقف.

-الثقة ليست بالضرورة أن تكون علاقة متعدية، حيث عندما يثق شخص (س) بشخص ثاني (ج)، ويثق (ج) بشخص آخر (ز)، فليس من الضرورة أن يثق (س)ـبـ(ز).

[1] سيد ماهر بدوي عبد الله، **المرجع السابق ذكره**، ص 49.

-الثقة تتميز بالتغيُر والتقلُب السريع، حيث يمكن أن تتغير ثقة شخص بشخص آخر بسرعة كبيرة لظرف أو لسبب من الأسباب.

-الثقة ليست تقدير أو تخمين أعمى، بل هي تقدير مبني على أساس الخبرة والتجارب والمعرفة السابقة، حيث أن الثقة هي عملية تنبُئية تعتمد على تجربة سابقة لنفس الشخص أو حالة مشابهة لشخص آخر.

-الثقة هي عملية ديناميكية مستمرة، حيث تزداد الثقة عندما تزداد التجارب الإيجابية للشخص وتنقص عندما تزداد التجارب السلبية للشخص.

❖ أهمية الثقة في البنوك الإلكترونية:

الوظيفة الأساسية للثقة تتمثل في الحد من عدم اليقين وتبسيط الاختيار، لذلك فالثقة مُهمة للعلاقات بين العملاء والبنك لعدة أسباب هي:[1]

-الثقة تُسهل المعاملات مع العملاء فلا يتعين عليهم القلق بشأن الاهتمام بمصالحهم الشخصية ومدخراتهم، وكذا المنتجات المالية التي تقدمها البنوك.

- ثقة الزبائن بالبنك هي تُحقق شعورا لديهم بأن البنك يخدم مصالحهم.

- المستوى العالي من الثقة يُعتبر بمثابة حاجز ضد التجارب السلبية التي يمكن أن تنشأ بين العملاء، حيث يميل العملاء إلى التغاضي عن التجارب السلبية باعتبارها استثناءً إذ كانوا يثقون في البنك، أما إذا كان مستوى الثقة منخفضا، قد ينظر إلى التجربة السلبية كدليل على عدم الوثوق في البنك.

- الثقة تساهم في إعطاء استمرارية العلاقة من خلال الرضا وخلق مشاعر الولاء، وبالتالي كلما زادت ثقة العملاء في المنشأة وموظفيها، زادت احتمالية مشاركتهم في تعاملات مستقبلية والحفاظ على علاقة طويلة الأمد معها.

-تساعد الثقة في جذب زبائن جدد والاحتفاظ بالزبائن الحاليين.[2]

- توفير الارتياح في العمل واتخاذ القرارات.

- تجعل علاقة التبادل مع العملاء طويلة الأمد ودائمة.

- تُعتبر الثقة عاملا حاسما لولاء العملاء، فهي تُحقق النجاح المستدام، وتعكس الرغبة في الاعتماد على الشريك، وتزيد من الدافعية المطلوبة للقيام بالسلوكيات الإيجابية، بالإضافة إلى تسهيل عمليات اتخاذ القرارات الشرائية المعقدة والتي تتصف بالتعقيد التكنولوجي والمخاطرة العالية، خاصة فيما يتعلق بالخيارات والقرارات المالية للعملاء، فهنا تلعب الثقة دورا هاما في الاختيار.

---

[1] سلمى بلمهدي، سمرة دومي، **دراسة مستوى ثقة الزبائن في البنوك التجارية–دراسة مقارنة بين البنوك العمومية والخاصة**، مجلة اقتصاديات الأعمال والتجارة، المجلد 6، العدد 2، 2021، ص 145.

[2] Kantsperger Roland, Werner Kunz, **Consumer Trust in Service companies: a Multiple Mediating analysis**, Managing Service Guality, Vol 20, N 01, 2010, P 9. https://doi:10.1108/09604521011011603.

-ثقة العملاء هي مُؤشر اقتصادي يقيس درجة تفاؤل العملاء فيما يتعلق بالحالة العامة لاقتصاد الدولة والأوضاع المالية الخاصة بهم، وهي مصدر حيوي للمعلومات الاقتصادية، إذ يُشكل الاستهلاك الخاص حوالي ثلثي النشاط الاقتصادي في معظم بلدان العالم، ومن المهم أيضا ملاحظة أن 81% من المتسوقين يوضحون أن الثقة تؤثر على قرارات الشراء الخاصة بهم.[1]

- الثقة مفتاح نجاح العلاقات التجارية لا سيما تلك التي تتميز بدرجة عالية من المخاطر، حيث يمكن اعتبارها كشبكة أمان.[2]

-الثقة هي الشرط الذي لا غنى عنه للاقتصاد الرقمي.[3]

-أكد Murph وGrundlach عن أهمية الثقة أنها: "المتغير الأكثر قبولا عالميا كأساس لأي تفاعل أو تبادل بشري"، وحسب Zeithaml: "أنها الأداة الوحيدة والأقوى المتاحة للشركة للتسويق بالعلاقات".[4]

-أشار Connolly إلى أن ثقة العميل أصبحت أكثر أهمية من أي وقت مضى، حيث لم تعد الوسائل التقليدية في السابق لبناء الثقة والحفاظ عليها فعالة بسبب العدد الهائل لمنصات الخدمات الإلكترونية المصرفية ووضعها التنافسي، لذلك أصبح لزاما على الشركات البحث عن طرقا جديدة لبناء ثقة العميل في هذه الخدمات.[5]

- وبالرغم من المزايا المذكورة أعلاه، فإن تعزيز الثقة لدى العملاء يُساهم في كسب ودهم وجذبهم من أجل استخدام الخدمات الإلكترونية المصرفية، لكن التواصل المباشر المادي الملموس (وجها لوجه) مع موظفي المصرف بواسطة قنوات التوزيع التقليدية المصرفية يبعثُ على الثقة والأمان والطمأنينة أكثر من التواصل الافتراضي غير المباشر بواسطة القنوات المصرفية الإلكترونية، وهذا ما يدعو لبذل المزيد من الجهود للرفع من آليات تعزيزها وجعلها بنفس المستوى.[6]

المطلب الرابع: أبعاد الثقة ومؤشرات وأدوات قياسها

قدم عدة باحثين سواء في مجال علم النفس الاجتماعي أو علم التسويق مجموعة من الأبعاد المكونة لمتغير الثقة وكل حسب منطلق موضوع بحثه واهتمامه، وهذا ما سنفصل فيه كالتالي:

---

[1] عامر عبد اللطيف، مصطفى صلاح عمر، أكرم نعيم قاسم، **تأثير التسويق الفيروسي في ثقة الزبون: دراسة تحليلية في شركة آسيا سيل**، مجلة التقنيات، المجلد 05، رقم 01، 2023، ص 197. https://doi.org/10.51173/jt.v5i1.1218

[2] Chris Halliburton, **The Role of Trust in Consumer Relationships**, ESCP Europe Business School, 2010, P 2.

[3] Tan Margaret, Teo Thompson, **Factors Influencing the Adoption of Internet Banking**, Journal of the AIS, Vol 1, N 5, 2000.

[4] https://shodhganga.inflibnet.ac.in/bitstream/10603/175638/4/13-chapter-5.pdf.22:30 تاريخ الاطلاع 08-08-2023، الساعة

[5] Connolly Barry, **Digital Trust: Social Media Strategies to Increase Trust and Engage Customers**, Bloomsbury Publishing, 2020.

[6] إبراهيم موصلي، **العوامل المؤثرة في سلوك العملاء تجاه الخدمات الإلكترونية للمصارف، دراسة ميدانية**، رسالة أعدت لنيل درجة ماجستير في إدارة الأعمال، جامعة حلب، كلية الاقتصاد، قسم إدارة الأعمال، 2011، ص 75.

❖ **أبعاد الثقة:**

اعتبر مفهوم الثقة خلال بدايات دراسته من قبل الباحثين على أنه بناء أحادي البعد، إذ يعتمد على تقييم الموثوقية الناشئة عن علم النفس الاجتماعي، غير أنه وعندما تم تناول الثقة ضمن حقل التسويق، تمت إضافة أبعاد أخرى لم يُتفق بشأن عددها أو طبيعتها، حيث أضاف Ganensen سنة 1994، بُعد المصداقية التي تُشير إلى الثقة الناتجة عن خبرة المؤسسة، وبُعد النفع الذي يُعبَر عن إيمان الزبون وقناعته باهتمام المؤسسة برفاهيته ومنفعته، إلا أن Gannon and Dony سنة 1997، قاما بانتقاد هذا الرأي باعتبار البُعدين مختلفين نظريا لكنهما لا ينفصلان عمليا، واقترحا الأبعاد الأربعة التالية: المصداقية، الموثوقية، التآلف، التوجه الذاتي، بتفسير ذلك أنه حين ترتبط المصداقية بالأقوال تظهر الموثوقية من خلال الأفعال، أما التآلف فيشمل جوانب العواطف والمشاعر، ليختص التوجه الذاتي بعنصر الدوافع،[1] وفي نفس الفكر التسويقي اقتراح الباحثين Mayer et al سنة 1995، تصنيف عام للثقة حيث رأوا أنها تتكون من ثلاثة أبعاد هي الأمانة (الموثوقية)، القدرة (الكفاءة)، النفع (الاحسان)، كما يلي:[2]

1-الموثوقية (Reliability): تشير الموثوقية إلى إدراك صاحب الثقة أن الموثوق به سيلتزم بمجموعة من مبادئ أو قواعد التبادل المقبولة لدى صاحب الثقة خلال وبعد عملية التبادل، فالموثوقية المدركة تغرس الثقة في سلوك الموثوق‌به وتخفض تصورات الخطر.

في مجال المعاملات الإلكترونية تشير قواعد الموثوقية إلى: أولا إجراءات المعاملات الإلكترونية، ثانيا سياسات خدمة العملاء بعد الصفقة، ثالثا استخدام الشركة للمعلومات والبيانات الخاصة بالمستخدم.

2-الكفاءة (Competence): هي مجموعة المهارات والقدرات والخصائص التي تُمكن طرف ما أن يكون له تأثير داخل مجال معين، فمجال القدرة يكون مُحددا لأن الموثوق به يمكن أن يكون لديه درجة عالية من الكفاءة في بعض المجالات الفنية، وتكفل أن يثق الزبون في المهام المرتبطة بهذه المجالات، وبالتالي فإن الثقة تكون محددة المجال Domain Specific، وقد أكَد الباحثون أن متغير الكفاءة هو عنصر ضروري للثقة.

وتشير الكفاءة لإدراك صاحب الثقة لقدرات ومعارف الموثوق فيه البارزة في السلوك المتوقع، هذه المدركات ربما تكون معتمدة على الخبرة السابقة أو الشهادات المؤسسية.

وفي مجال المعاملات الإلكترونية إدراك كفاءة الشركة أو المؤسسة يعتمد على اعتقادين مرتبطين هما: أولا ما إذا كانت الشركة أو المؤسسة كفء ولديها خبرة ومهارات بدرجة كافية لأداء السلوك المقصود، وثانيا ما إذا كانت الشركة أو المؤسسة لديها فرص الحصول على المعارف اللازمة لأداء السلوك بشكل مناسب أو ملائم،

---

[1] سعدية مزيان، **أثر ثقة الزبائن على ولائهم للمؤسسات الصحية الخاصة، دراسة حالة عينة عيادة نوميديا أم البواقي**، مجلة جديد الاقتصاد، المجلد 17، العدد 01، 2022، ص 379.

[2] سيد ماهر بدوي عبد الله، **أثر ثقة العميل في المؤسسة المصرفية على قبول التعامل المصرفي عبر الإنترنت**، رسالة ماجستير، كلية التجارة، قسم إدارة الأعمال، جامعة القاهرة مصر، 2013، ص 61.

وبالتالي الكفاءة تكون محددة المجال، فالموثوق بهم المهرة في مجال معين ينظر إليهم بأنهم لديهم كفاءة أو خبرة قليلة في المجالات الأخرى.

3-النفع (Benevolence): يُشير إلى النفع إلى أن الموثُوق به يكون مُحسنا لصاحب الثقة حتى وبعد انتهائه من تقديم الخدمة، فالنفع يُقدم إيمان وإيثار في العلاقة، ويُقلل من عدم التأكد والميل للحذر من السلوك الانتهازي المضاد، وفي مجال التعاملات الإلكترونية قد يكون مكلف جدا تصميم الخدمات الخيَرة أو النافعة، ففي مثل هذه الظروف يجب على المؤسسة أن تعمل على: أولا إبداء التعاطف والقابلية نحو اهتمامات وحاجات المستخدمين، ثانيا عمل جهود بحسن نية لحل مشاكل المستخدم.

إن الموثوقية، الكفاءة والنفع كلها عوامل هامة للثقة، وكل منها قد يختلف بشكل مستقل عن الآخر ولكن هذا لا يعني أنها عوامل ليست مرتبطة ببعضها، فهذه العوامل كمجموعة تبدو أنها تُفسر جزءً كبيرا من **الجدارة بالثقة (Trust worthiness)**، وعليه حين يُدرك صاحب الثقة أن الموثوق به تتوافر فيه هذه العوامل بدرجة عالية فيمكن القول بأن هذه المؤسسة هي جديرة بالثقة تماما.

بعد مراجعة العديد من الدراسات السابقة، هذه الأبعاد الثلاثة مختلفة من الناحية المفاهيمية، حيث تدخل فيها عدة عناصر مختلفة من خلاصة الثقة المعرفية والثقة العاطفية، وهي تمثل مساحة البعد الشامل لتشكيلة وصياغة الثقة، وهذا ما جاء به كل من Richardson and Swan, Bowers سنة 1999، حيث جعلوا مختلف المتغيرات السالفة الذكر في بعدين أساسيين للثقة، هما: **البعد المعرفي، والبعد العاطفي**، وغالبا ما يتم اعتماد هذا المفهوم الثنائي في مجال التسويق لأبعاد الثقة عند دراسة العلاقة بين (B to C) سواءً كانت ثقة شخصية أو ثقة المؤسسة، حيث يتمثل هاذين البعدين في:[1]

1-البعد المعرفي (Cognitive Dimension): وهو اعتقاد بأن الشريك لديه الخبرة والمهارة بمعنى (الكفاءة) والدوافع الضرورية لتأمين شرط التعامل، فهذا البعد ذو طبيعة فنية، وهو يقود العملاء للوثوق في حدوث رضا في المستقبل وأن الموثوق فيه يفي بالوعود ويُلبي الاحتياجات.

2-البعد العاطفي (Emotional Dimension): يتعلق بالصدق والأمانة أو درجة الاحسان للشريك، حيث أن صديق الشريك هو الوعد بالاحترام والالتزام بشروط التبادل بمعنى (الموثوقية)، ويتعلق أيضا بالإحسان الذي يُشير إلى الشعور بالأمان حول قدرة الاعتماد على الأشخاص الذين هم على اتصال والذين سيأخذون بعين الاعتبار مصلحة الشريك من خلال نفعه (النفع)، وأن الموثوق فيه يُريد الأفضل لمنح الثقة بغض النظر عن دافع الربح، فهذا البعد يصف جانب الاعتقاد الذي يتجاوز توافر الأدلة لجعل العملاء يشعرون بأن الموثوق فيه سوف يكون مسؤول وراعي لهم على الرغم من تقلبات الأوضاع والظروف المستقبلية.

[1] Lynne Richardson, John Swan, Michael Bowers, **Customer Trust in The Salesperson: An Integrative Review and a Meta-Analysis of The Empirical Literature**, Journal of Business Research, Vol 44, 1999, P 93-107.

وهذا ما تم تأكيده في دراسة: Shaqrah et al، سنة 2011، إذ تعد الثقة مفهوما متعدد الأبعاد في طبيعته، ليتم جمعها في بعدين أساسيين هما:[1]

1-الثقة على أساس المعرفة: ويُقصد بها النظرة العقلانية للثقة، التي ترتبط بإدراك العميل للكفاءات، والقدرة، والمسؤولية، والسلامة، والمصداقية، والموثوقية، ويندرج ضمنها الثقة المحسوبة التي ترتبط بفكرة العائد والتكلفة.

2-الثقة على أساس العاطفة: وهي أكثر ارتباطا بالعاطفة والأكثر تأثيرا، بحيث تتضمن عدة عوامل مثل: العناية، والاهتمام، والإحسان، والايثار، والالتزام، والاحترام المتبادل، ويندرج ضمنها الثقة غير المحسوبة التي ترتبط بمواقف الأفراد وقيمهم.

ونفس الشيء بالنسبة لدراسة: Barclay وSmith سنة 2015،[2] ودراسة: Doumi, Belmahdi، سنة 2021،[3] الذين تحدثوا عن الثقة على أنها: "توقعات معرفية (البعد المعرفي)، وإحساس شعوري (البعد العاطفي)".

وعليه، اعتمدنا في نموذج دراستنا الحالية لأبعاد المتغير الوسيطي (ثقة العملاء) على هاته الدراسات السابقة، استنادا إلى مؤشرات مقاييسها المرتبطة بالمفهوم الثنائي.

❖ مؤشرات مقياس ثقة العملاء:

يُعتبر قياس الثقة أمرا مهما بالنسبة لأي مؤسسة، لأنه يُعبر عن مدى نجاحها في التعامل مع عملائها وفي تسويق خدماتها، ومدى ثقتهم عما تقدمه من خدمات، حيث قدم العديد من الباحثين مقاييس من أجل تقييم ثقة العملاء في خدمات المؤسسة، وأحد أهم تلك المقاييس هو مقياس ثقة العملاء المبني على قياس أبعاد الثقة ومكوناتها، ويتكون هذا المقياس من المؤشرات التالية:[4]

-الإعلان حول منتجات أو خدمات المؤسسة يمنح العملاء مستوى مرضي من الأمان.

-الإعلان حول علامة منتجات أو خدمات المؤسسة يمنح العملاء مستوى مرضي من الثقة.

-شراء منتجات أو استخدام خدمات المؤسسة يمنح العملاء مستوى مرضي من الضمان.

---

[1] Amin Shaqrah, Read Alqirem, Khaled Alomoush, **Affecting Factors of Knowledge Sharing on CRM: An Empirical Investigation Using Structural Equation Modeling**, World Journal of Social Sciences, Vol 01, N 01, 2011, P 03.

[2] بن أشنهو محم، قريش بن علال، **العوامل المؤثرة على ثقة الزبون، دراسة إمبريقية باستعمال طريقة المعادلات البنائية**، مجلة المالية والأسواق، المجلد 02، العدد 02، 2015، ص 07.

[3] سلمى بلمهدي، سمرة دومي، **المرجع السابق ذكره**، ص 145.

[4] عمر توفيق عبد الرحيم، ثابت حسان ثابت، عمر سالم عز، **تحليل العوامل المؤثرة على تعزيز ثقة الزبون في استخدام الخدمات المصرفية الذكية: تطبيقات الهواتف الذكية أنموذجا**، مجلة العلوم المالية والمحاسبة، 2022، ص 546.

-إن المؤسسة وفية تجاه ثقة العملاء الممنوحة لخدماتها.

- إن المؤسسة صادقة تجاه متطلبات عملائها.

-إن المؤسسة تمنح عملائها الفائدة المرجوة منها.

- إن المؤسسة تحدَث خدماتها وفق التطورات المتسارعة في المجتمع والبيئة.

-إن المؤسسة تحسن خدماتها بشكل مستمر من أجل تلبية احتياجات عملائها.

❖ أدوات قياس ثقة العملاء:

تُقاس ثقة العملاء اعتمادا على مجموعة من الأدوات هي:[1]

1-المسح الميداني: من خلال مسوح دورية يُستخدم فيها الاستبيان لقياس مستوى الثقة لدى العملاء، وذلك من خلال مجموعة من الأسئلة والعبارات المرتبة وترسل للأشخاص المعنيين عبر البريد أو يجرى تسليمها باليد.

2-نظام الشكاوى والمقترحات: وهي عبارة عن توقعات العملاء التي لم تقم المؤسسة بإشباعها وهي سلاح ذو حدين إذا تم الاهتمام بها زاد ولاء العملاء والعكس، حيث تُتيح العديد من المؤسسات نظام يسهل على العملاء تقديم شكاوى واقتراحات للمؤسسة، سواء من خلال إتاحة بريدي إلكتروني أو موقع تتلقى من خلاله شكاويهم.

3-المقابلات الشخصية والاتصال بالعملاء الحاليين: يقوم بها مدراء وممثلي المؤسسة المكلفين بهذه المهمة، فالمقابلة عبارة عن محادثة يقوم بها شخص متخصص مع فرد أو أفراد بهدف حصوله على مجموعة من المعلومات التي يريدها، وهي تعتبر أكثر وسائل جمع المعلومات، بالإضافة إلى قدرة المقابلة على فهم وتحليل سلوك الفرد المقابل بصورة كبيرة وذلك بسبب الاتصال المباشر، فعملية المشارك في النقاش توفر عنصر التغذية العكسية مباشرة حيث يتاح للمقابل فرصة أكبر لتغطية الموضوع والاستفسار عن كل شيء من الشخص المستقصي منه.

4-الاستبيان (البريد المباشر): يتم من خلال إعداد قائمة بالأسئلة في شكل استبيان يوجه للعميل ليقوم بملئه على انفراد دون تدخل المستجوب، يتم ارسال الاستبيانات عن طريق البريد أو الإنترنت أو تسليمها باليد، وتتميز هذه الطريقة وهي الأكثر استعمالا في مجال المنتجات الواسعة الاستهلاك بالنظر إلى حجم العينة الذي يكون كبير وبالتالي لا تكون مكلفة.

5-بحوث العملاء المفقودين: تكون من خلال تشخيص للعملاء المفقودين عن طريق تحليل أسباب توقفهم عن التعامل مع المنظمة ومحاولة إزالة هذه الأسباب والعمل على تحقيق ثقتهم من خلال الاتصال بالعملاء الذين تحولوا عن التعامل مع المنظمة، وهذا من أجل معرفة ومراقبة أسباب امتناعهم ومحاولة تقليل معدلات فقدانهم.

6-تحليل شرائح العملاء وشخصياتهم: كلما عرفت المزيد عن الأنماط الشخصية لشرائح عملائها زادت معرفة المؤسسة بنوعية الخدمات أو أساليب المعاملة التي تحقق لهم الثقة وذلك دون توجيه سؤال لهم.

[1] عمار بوحوش، محمد الذنيبات، **مناهج البحث العلمي وطرق إعداد البحوث**، الطبعة السادسة ديوان المطبوعات الجامعية بن عكنون، الجزائر، 2018، ص 71.

المطلب الخامس: مراحل بناء ثقة العملاء وطرق تعزيزها

بشكل عام تتشكل الثقة في مزود الخدمة من خلال وجهين متميزين هما الثقة في الموظفين والثقة في المؤسسة، وتتشكل الثقة في الموظفين من خلال تصورات سلوك الموظفين التي تظهر أثناء اللقاء الخدمي، في حين أن الأحكام المتعلقة بالثقة في المؤسسة تستند أساسا إلى السياسات والممارسات التي تحكم التبادل.

❖ مراحل بناء ثقة العملاء:

حيث حدّد كل من Gatfaoui de Shéraza ثلاثة مراحل أساسية لبناء الثقة في العلاقات التي تقوم بين العملاء والبنوك الالكترونية الخاص بهم، وهي كالتالي:[1]

- المرحلة الأولى: فترة ما قبل الدخول في علاقة مع البنك الالكتروني:

في هذه المرحلة ينظر العملاء بشكل أساسي إلى الثقة المؤسسية لتبرير اختيار الدخول في علاقة مع البنك، هذا واضح لأن العميل لم يختبر بعد العلاقة مع البنك مقدم الخدمة، وهنا تأتي الثقة من عملية معرفية مرتبطة بمعرفة البنك من خلال الاتصال سواء: (الصحافة، التلفزيون، الإنترنت، اللوحات الإعلانية، الراديو، ...إلخ) أو العائلة أو الأصدقاء (الكلمة المنطوقة)، كما تعتمد الثقة المؤسسية على سمعة البنك، وحجمه وخبرته.

- المرحلة الثانية: الفترة المتعلقة بتجربة الخدمة الأولى مع البنك الإلكتروني:

تُعتبر التجربة الأولى للعملاء مع البنك عاملا حاسما في تعزيز الثقة المؤسسية ودفع العملاء نحو الثقة الشخصية، فالتجربة الأولى الإيجابية تولد ثقة شخصية تنعكس بشكل إيجابي على الثقة المؤسسية، أو قد يحدث العكس تماما نتيجة فشل اللقاء الخدمي الأول بين العميل ومقدم الخدمة، وفي هذه المرحلة يكون لمقدم الخدمة البنكية الدور الرئيسي لتعزيز الثقة لدى العملاء من خلال السلوكيات الصادرة عنه وكفاءته، مثلا: تقدُم العميل لاستلام بطاقة الائتمان وتزويده بالرقم السري لها، وتحسيسه بطرق المحافظة على السرية والخصوصية....إلخ، بغية تعزيز ثقته.

– المرحلة الثالثة: خلال تجارب الخدمة المتكررة:

طوال العلاقة المصرفية من خلال تجارب الخدمة المتكررة مع البنك يمكن أن تستند الثقة على مصداقية البنك والشعور بأن العملاء يمكنهم الاعتماد عليه في حالة مواجهتهم لصعوبات مالية مستقبلية، وفي هذه المرحلة يمكن اعتبار الثقة الشخصية (علاقة العميل مع مقدم الخدمة) أكثر أهمية من الثقة المؤسسية (علاقة العميل مع البنك). فتُساهم عدة عوامل في بناء الثقة واستمرارها مثل صدق وشفافية مقدم الخدمة، التواصل الجيد مع العميل

[1] Santos, Cristiane Pizzutti, **Antecedents and consequences of consumer trust in the context of service recovery**, Brazilian Administration Review, Vol 5, N 3, 2008, p 227. https://doi.org/10.1590/s1807-76922008000300005.

والتفاعل معه وحسن الاستماع إليه، الاحسان إلى العميل ومراعاة مصلحته، التعرف عليه، إيجاد حلول لمشاكله، خبرة وكفاءة مقدم الخدمة، التجارب السابقة مع مقدم الخدمة، والتجارب مع البنك، وسمعة البنك وحجمه وخبرته.

❖ طرق تعزيز ثقة العملاء:

تُعتبر ثقة العملاء بالغة الأهمية للمؤسسة، وذلك لأنها لا تساهم في تحولهم إلى عملاء دائمين فحسب، بل وأكثر من ذلك، فإنهم سيذكرون تجاربهم الناجحة أمام أصدقائهم، ما يضمن توالي أرباحها ونموها بشكل كبير، لذلك تسعى المؤسسة لكسب ثقتهم بشتى الطرق، نذكر منها:[1]

-تقديم الحلول ومعالجة الشكاوى، لأن ذلك سيؤدي إلى شعور العملاء بالأمان.

-توضيح مزايا المنتج بدون مبالغة، لتجنب رفع مستوى توقعات العملاء يفوق المنفعة المدركة.

-تجنب الوعود الكاذبة، لأنها تؤثر على سمعة المؤسسة.

-تقديم العروض الخاصة، لأنها تشجع العملاء على تكرار الشراء.

-خدمات ما بعد البيع، والتي تُعد من أهم أسرار كسب ثقة العملاء وتحولهم إلى دائمين.

-التنبؤ مسبقا باحتياجات العملاء ومتطلباتهم، بغرض توفيرها وفق توقعاتهم.

-السماع إلى ملاحظات العملاء والسعي لتطبيقها عمليا.

-التحلي بالوضوح والشفافية مع العملاء، مع إظهار التعاطف معهم ومشاركة تجاربهم.

-جعل تجربة الشراء أو تقديم الخدمة سهلة الاستخدام، مع الاعتراف في حال وجود أخطاء تواجه العملاء.

-التنبؤ مسبقا باحتياجات العملاء ومتطلباتهم، بغرض توفيرها وفق توقعاتهم.

-الحرص على التواصل الدائم كإنشاء قسم خاص بخدمة العملاء، يهدف إلى خدمتهم بطريقة سريعة وفعَالة.

-بناء علاقات وطيدة للاحتفاظ بالعملاء وتعزيز ثقتهم، ذلك يُبرز مدى الاهتمام بهم، كتهنئتهم في المناسبات.

المبحث الثاني: الخدمات الإلكترونية المصرفية (Electronic Banking Services)

أدت ثورة تكنولوجيا الاعلام والاتصال في عصر التطورات المتلاحقة إلى ظهور تغيرات جوهرية في الاقتصاد، فظهر الاقتصاد الرقمي الذي يعتمد على التقنية، ما أدى إلى إفراز عدة مصطلحات جديدة من بينها: التجارة الإلكترونية، البنوك الإلكترونية، التسويق الرقمي، ...الخ، لتُصبح بذلك سمة من سمات الدول المتقدمة وبروز التفاوت الكبير بينها وبين دول العالم الثالث، فهذا التفاوت سُمي بالفجوة الرقمية، كما أصبحت اقتصاديات الدول تُقاس في تطورها بمدى توجُهها نحو رقمنة اقتصادها.

[1] الموقع: https://blog.araboost.com/influencers-marketing-stratistics، تاريخ الاطلاع: 16-06-2023، على الساعة 20:30.

ومن بين الركائز الأساسية التي يقوم عليها الاقتصاد الرقمي هي البنوك، من خلال ما تقدمه من خدمات إلكترونية مختلفة لكافة الهياكل والقطاعات الأخرى، وبهذا سيتم التطرق بالتفصيل حول المفاهيم المتعلقة بالخدمة المصرفية الإلكترونية.

المطلب الأول: تعريف الخدمات الإلكترونية المصرفية ودوافع ظهورها

هناك عدة تعاريف للخدمة الإلكترونية المصرفية، ومجموعة من الدوافع والأسباب التي أدت إلى ظهورها كما يلي:

❖ تعريف الخدمات الإلكترونية المصرفية:

يُقصد بالخدمات الإلكترونية المصرفية: "تقديم البنوك للخدمات المصرفية التقليدية أو الحديثة من خلال شبكات اتصال إلكترونية، تقتصر صلاحية الدخول إليها على المشاركين فيها وفقا لشروط العضوية التي تحددها البنوك، وذلك من خلال أحد المنافذ على الشبكة كوسيلة لاتصال العملاء بها بهدف:[1]

-اتاحة المعلومات عن الخدمات التي يؤديها البنك.

-حصول العملاء على خدمات محدودة كالتعرف على معاملاتهم وأرصدة حساباتهم وتحديث بياناتهم وطلب الحصول على القروض.

-طلب العملاء تنفيذ عمليات مصرفية مثل تحويل الأموال.

فالخدمات الإلكترونية المصرفية هي تشمل المعاملات المالية بين المؤسسات المالية والأفراد والشركات التجارية والحكومية، ومن أجل الربحية تحاول المنظمات المصرفية كالمنظمات الأخرى السيطرة على التكاليف وخفض المصروفات التشغيلية، متخذة من التكنولوجيا والابتكار أدوات لتحقيق ذلك، حيث يستطيع العميل انطلاقا من حاسوبه الشخصي الذي يتم ربطه بحواسيب البنك عبر الخطوط الهاتفية القيام بمختلف العمليات المصرفية، وهذا ما يزيد كثيرا من راحة العملاء حيث لا تُوفر الخدمات الإلكترونية المصرفية عليهم عناء التنقل فقط، بل تجعل استخدام الموزع الآلي والصيرفة الهاتفية والصيرفة بالمراسلة في أغلب الحالات عمليات ضرورية تُكسبهم الجهد والوقت، كما يمكن أيضا من اجراء العمليات ليس فقط على مستوى محلي، بل على مستوى عالمي دون انقطاع، ويستخدم العميل برنامج إدارة الأموال الشخصية وحاسوبه الخاص، بالإضافة إلى مودم وخط هاتفي للدخول إلى البنك وإجراء العمليات المصرفية.[2]

---

[1] صليح بونفلة، **النظام القانوني للعمليات المصرفية الإلكترونية**، أطروحة مقدمة لنيل شهادة الدكتوراه تخصص قانون الأعمال، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة 8 ماي 1945 قالمة، الجزائر، 2021، ص 32.

[2] بن صالح ماجدة، أطروحة دكتوراه، **نفس المرجع السابق**، ص 96.

وللتوضيح أكثر، قدم كوه وآخرون (Koh et al) تعريفا للخدمات المصرفية الإلكترونية بأنها: "نماذج الأعمال الناشئة التي تحركها البيانات الضخمة وسلاسل الكتل والذكاء الاصطناعي والحوسبة السحابية وغيرها من التقنيات الحديثة في الأسواق المالية".[1]

أما Amos Olushola Michael، عرفها على أنها: "عبارة عن تقديم المنتجات والخدمات المصرفية إلكترونيا مباشرة إلى العملاء أينما كانوا، وقد تكون خدمات عبر الإنترنت، خدمات افتراضية، خدمات عبر الكمبيوتر الشخصي، خدمات منزلية، خدمات عن بعد، وخدمات مصرفية عبر الهاتف، ويتم استخدام العديد من المصطلحات لوصف الخدمات الإلكترونية المصرفية، وغالبا يتم استخدامها بالتبادل".[2]

وأضاف دسيلفا وآخرون (D'Silva and al) أن المميزات الرئيسة لاستخدام الخدمات الإلكترونية المصرفية تتمثل في القُدرة على استخدامها عبر الأجهزة المحمولة وإمكانية التعرف على الهوية بشكل سريع، كما أنها سريعة الانتشار بين مئات الملايين من العملاء، ويمكن استخدامها في المعاملات المالية منخفضة القيمة أو مرتفعة القيمة، بالإضافة إلى تكلفتها المنخفضة في الاستخدام.[3]

على العموم، يمكن أن نستخلص أن الخدمات الإلكترونية المصرفية هي الخدمات أو الوسائل المتطورة الحديثة التي تستخدمها البنوك في وقتنا الحالي لأداء عملياتها المصرفية بأقل تكلفة وأقل جهد وبفعالية أكثر، وهذا لإشباع حاجات ورغبات عملاءها، بحيث يمكن هذا الأخير القيام بالأعمال المصرفية التي يريدها إلكترونيا في أي زمان ومكان دون الحاجة لتنقله إلى المصرف.

❖ دوافع ظهور الخدمات الإلكترونية المصرفية:

يجب الإشارة إلى أن "ظهور الخدمات الإلكترونية المصرفية ارتبط بظهور النقد الإلكتروني في بداية ثمانينيات القرن الماضي، حيث برز مفهوم (La Monétique) الذي يعني تزاوج النقد بالإلكترونيك".[4]

وهذا الظهور كان نتيجة تفاعل عدة عناصر منها:[5]

-ثورة تكنولوجيا المعلومات والاتصال أدت إلى ظهور تغيرات جوهرية في طبيعة عمل القطاع المصرفي المالي.

---

[1] **Koh Francis**, **Phoon Kok**, **Ha Cao**, Digital Financial Inclusion in South East Asia, In Hondbook of Blockchain, Digital Finance, and Inclusion, **Academic Press**, **Vol 2**, **2018**, **P 387**.

[2] Amos Olushola Michael, **The Effect of Electronic Banking on Bank Performance in Nigeria**, **European Journal of Business and Management**, Vol 12, N 26, 2020, P 79.

[3] D'Silva Derryl, Filkova Zuzana, Packer Frank, Tiwari Siddharth, **The Design of digital Financial Infrastructure**: **Lessons from India**, BIS Paper, 2019, P 106.

[4] مخرمش حاج محمد، **دور الصيرفة الإلكترونية في تحقيق الميزة التنافسية للبنوك التجارية**، مذكرة مقدمة لاستكمال متطلبات شهادة ماجستير أكاديمي تخصص مالية وبنوك، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة ورقلة، الجزائر، 2018، ص 02.

[5] أحمد سفر، **العمل المصرفي الإلكتروني في البلدان العربية**، المؤسسة الحديثة للكتاب، طرابلس، لبنان، دون طبعة، 2006، ص 64.

-التجارة الإلكترونية التي تتم باستخدام الوسائل الإلكترونية وخاصة الإنترنت، والتي أصبحت تتميز بخصائص عديدة تميزها عن التجارة التقليدية خاصة في إستراتيجيات وأساليب عمل البنوك.

-وجود منافسة شديدة بين البنوك مع بعضها البعض ومع غيرها من المؤسسات المالية، حيث اكتسبت هاته المنافسة أبعاد دولية في تحرير التجارة العالمية.

-تزايد دخول العديد من المؤسسات المالية غير المصرفية مثل: شركات التأمين وشركات الأوراق المالية ومنافستها للبنوك، حيث أصبح العديد من هاته المؤسسات يقدم مجموعة خدمات وثيقة الصلة بعمل البنوك.

-وجود تطوير الأداء بصفة مستمرة سواء للبنوك أو غيرها من المؤسسات المالية لرفع مستوى الكفاءة التشغيلية والنفقة لتُقدم أفضل خدمة لعملائها، وبالأخص أن الكثير من العملاء خاصة المؤسسات أصبحوا يطلبون خدمة رفيعة المستوى بتكلفة تنافسية، مستفيدين من المنافسة المتزايدة بين المؤسسات.

عليه، نستنتج أن تغير الظروف والأحوال يتبعُه تغير الأدوات والوسائل، إذ لا يجوز استخدام وسائل تقليدية في عصر ظهرت فيه التقنيات، وأصبحت مؤشرات يُقاس بها تطور الدول ومؤسساتها، مثلما هو الحال في العمل المالي عامة والمصرفي خاصة.

المطلب الثاني: أهمية ومزايا الخدمات الإلكترونية المصرفية

للخدمات الإلكترونية المصرفية أهمية كبيرة في وقتنا الحالي، نظرا لما تحمله من سمات ومزايا عديدة هي كالآتي:

❖ أهمية الخدمات الإلكترونية المصرفية:

أصبحت الخدمات الإلكترونية المصرفية تمثل الركيزة الأساسية للصناعة المصرفية، والعنوان الرئيسي للتعاملات المستقبلية والتي ستُمكن العملاء من إتمام غالبية عملياتهم واحتياجاتهم دون الحاجة لزيارة فرع المصرف، لذا أدركت المصارف المعاصرة أهمية تحقيق الترابط بين نجاح البنك وتوجهه الإبداعي في مجال توظيف التكنولوجيا واستثمارها في التعرف على احتياجات العملاء والسعي لتحقيق أعلى مستويات الاشباع لرغبات العملاء.

كما أسهمت الخدمات الإلكترونية المصرفية في الارتقاء بمعايير وجودة الخدمات المصرفية، وأتاحت قدر أوسع من الفعالية في تنفيذ العمليات بشكل فوري ومباشر، فضلا عن اتساع مظلة الخدمات التي بات من الممكن تنفيذها بواسطة القنوات المصرفية الإلكترونية المختلفة، إلى جانب ما أسهمت به تلك القنوات من رفع معدلات الحماية وتقليص احتمالات الأخطاء التشغيلية التي قد تحدُث من العنصر البشري، إذ أن كافة الخدمات الإلكترونية هي تخضع لسلسلة دقيقة من الإجراءات ومراحل التدقيق للتأكيد على سلامة عملياتها.[1]

[1] راحو بلال، **الخدمات المصرفية الإلكترونية وأثرها في تحسين جودة الخدمات المصرفية الإلكترونية، دراسة تطبيقية لأراء عينة من الزبائن والإداريين العاملين بالمصارف التجارية العاملة في مدينة البليدة**، رسالة ماجستير في العلوم الاقتصادية، تخصص مالي ونقود، جامعة الدكتور يحي فارس المدية، الجزائر، 2015، ص 28.

ويمكن أن تظهر أهمية الخدمات الإلكترونية المصرفية من ناحية البنوك، ومن ناحية العملاء، وهي كما يلي:[1]

أولا: أهمية الخدمات الإلكترونية المصرفية من ناحية البنوك:

✓ **تحقيق الميزة التنافسية:** يكون هذا من خلال تمكينها من التعامل مع الأسواق المستهدفة وعناصر البيئة المحيطة بها بصورة أفضل، حيث الهدف الأساسي هو كسب عدد أكبر من العملاء والحافظ عليهم.

✓ **تحقيق الربحية في الأجل الطويل:** يساهم استخدام الخدمات المصارف للأنظمة الإلكترونية في تحقيق معدلات ربحية، وهذا من خلال انخفاض تكلفة الخدمات الإلكترونية المصرفية، فالمعاملات الإلكترونية هي أرخص طرق المعاملات (انخفاض التكاليف الثابتة خاصة للفروع)، وارتفاع ربحية قطاع عملاء الصيرفة الإلكترونية بسبب انخفاض حساسيتهم السعرية إذا ما قورنت بعملاء الخدمة المصرفية التقليدية.

✓ **توفير فرص تسويقية جيدة:** يتيح نظام توزيع الصيرفة الإلكترونية من خلال برامج البحث إمكانية أكبر للعملاء لإجراء عمليات التسويق الإلكتروني.

✓ **توزيع واسع الانتشار:** تهدف الأنظمة الإلكترونية الحديثة إلى تغطية واسعة الانتشار حتى تصل الخدمة للعميل في أي مكان، فيستطيع بذلك الحصول على ما يرغب من خدمات مصرفية دون الحاجة إلى الانتقال إلى مبنى المصرف أو الوقوف المطول في طوابير الانتظار.

✓ **تحسين جودة الخدمة المصرفية:** من خلال إدخال واستعمال الأساليب والتقنيات التكنولوجية الحديثة التي تعمل على تطوير الخدمات المصرفية، وكسب رضا وثقة العملاء.

✓ **هامش منخفض للخطأ البشري:** تساعد الخدمات الإلكترونية المصرفية في تقليل الأخطاء المختلفة مقارنة بالمعاملات المصرفية العادية.

✓ **تقلل السجلات:** الخدمات الإلكترونية تقلل الأعمال الورقية وتجعل العملية أسهل في التعامل معها.

✓ **تدفع إلى زيادة مستوى ولاء العملاء:** الخدمات الإلكترونية المصرفية هي تعمل على تحقيق الرضا بما ينمي الثقة ويخلق الولاء لدى العملاء ما ينتج عنه استمرارية ربح المؤسسة.

✓ **الحد من الاحتيال:** حيث تقدم الخدمات الإلكترونية المصرفية البصمة الرقمية لجميع الموظفين الذين لديهم الحق في تعديل الأنشطة المصرفية.

ثانيا: أهمية الخدمات الإلكترونية المصرفية من ناحية العملاء:

✓ **الراحة:** حيث يمكن للعميل الوصل إلى حسابه والتعامل من أي مكان 24/24 سا وخلال مدار أيام الأسبوع وحتى في مختلف العطل.

[1] Arya Himanshu, **E-Banking**: **The Emerging Trend**, International Journal of Trend in Scientific Research and Development IHTSRD, Vol 3, N 4, Jun 2019, P 452. https://doi:10.31142/ijtsrd23689.

✓ **تكلفة أقل لكل معاملة:** لأن العميل لا يتوجب عليه زيارة الفرع في كل معاملة، مما يوفر له الوقت والجهد والمال.

✓ **تقليل الحواجز الجغرافية:** نقصد بالتي يمكن أن تُعيق بعض المعاملات المصرفية.

✓ **سهولة مراجعة نشاط الحساب:** يمكن لرجال الأعمال والعملاء الوصول إلى الحسابات بسرعة باستخدام ملف واجهة الخدمات المصرفية عبر الإنترنت، وهذا ما يسمح لهم بمراجعة نشاط الحساب، وكذلك ضمان حسن سير العمل من الحساب وتسجيل كل أثر للعمليات المصرفية.

❖ مزايا الخدمات الإلكترونية المصرفية:

يكتسي العمل المصرفي الإلكتروني جملة من المزايا شأنه شأن الأنشطة الأخرى، حيث تسمح الصيرفة الإلكترونية بتقديم خدمات حديثة تُميزها عن خدمات الصيرفة التقليدية، ومن أهم المزايا التي تتسم بها:[1]

1-إمكانية الوصول إلى قاعدة أوسع من العملاء: حيث تتميز الصيرفة الإلكترونية بقدرتها على الوصول إلى قاعدة عريضة من العملاء ودون التقيد بمكان أو زمان معين، كما تتيح لهم إمكانية طلب الخدمة في أي وقت وطوال أيام الأسبوع وهو ما يوفر الراحة للعميل، إضافة إلى سرية التعامل والتي تزيد من درجة ثقتهم في البنك.

2-تقديم خدمات مصرفية متكاملة وجديدة: حيث تتضمن الصيرفة الإلكترونية كافة الخدمات المصرفية التقليدية وإلى جانبها خدمات أكثر تطورا عبر الوسائل التقنية الحديثة مثل:

- إصدار النشرات الإلكترونية الاعلانية عن مختلف الخدمات المصرفية.
- إعداد العملاء بطريقة التأكد من أنشطتهم لدى المصارف.
- تقديم طريقة دفع العملاء للكمبيالات المسحوبة عليهم إلكترونيا.
- كيفية إدارة الحافظة المالية من أسهم وسندات للعملاء.
- تحرير العملاء من قيود الزمان والمكان.
- القدرة على الحصول على المعلومات المطلوبة عن طريق الإنترنت.
- الحصول على نصائح مالية من المصرف سواء من خلال البريدي الإلكتروني أو بشكل مرئي من خلال الكاميرات.
- طريقة تحويل الأموال بين حسابات العملاء المختلفة.

3-خفض التكاليف: من أهم ما يُميز الخدمات الإلكترونية المصرفية هو أن تكاليف تقديم الخدمة منخفضة مقارنة بأعمال الصيرفة التقليدية، ومن ثم فإن التكلفة وتحسين جودتها هو من عوامل جذب العملاء، فتبين نتائج

[1] أحمد بوراس، سعيد بريكة، **أعمال الصيرفة الإلكترونية الأدوات والمخاطر**، دار الكتاب الحديث، القاهرة، مصر، الطبعة الأولى، 2014، ص 134.

المقارنة بين العمل المصرفي الإلكتروني والتقليدي بأن تكلفة تقديم الخدمات في القنوات الإلكترونية أقل بنحو ستة مرات عنها في القنوات التقليدية للعمل المصرفي، وأن نسبة التوفير في التعاملات المصرفية الإلكترونية تقدر بنحو 35% للمعاملات المصرفية عبر الإنترنت عنها في الأنماط التقليدية.

4-سرعة إنجاز الأعمال المصرفية: مع اتساع وسائل التقنية الحديثة وما أحدثته من سرعة في إنجاز الأعمال المصرفية، أضحى سهلا على الزبون الاتصال بالمصرف، وأن يقوم بتنفيذ الإجراءات التي تنتهي في أجزاء صغيرة من الدقيقة، بكفاءة عالية وأداء صحيح دون عناء التنقل شخصيا لأداء نشاطه المطلوب.

5-توسيع الخيارات: عموما تُتيح الصيرفة الإلكترونية حرية أكثر في اختيار الخدمات ونوعيتها، وخيارات أوسع للمتعاملين بها.

6-تسهيل على العملاء مقارنة خدمات ومنتجات البنوك: مما زاد من المنافسة بينها وسمح لها باختراق أسواق جديدة ووسع انتشارها الجغرافي.

7-الطبيعة الدولية: تتسم الخدمات الإلكترونية المصرفية بالطبيعة الدولية، أي أنها مقبولة من جميع الدول، ويتم استخدامها لتسوية الحسابات في مختلف المعاملات عبر الفضاء الإلكتروني بين المستخدمين وعبر أنحاء العالم.

8-توفير الخدمة في الوقت الحقيقي: توفر البنوك عن طريق تبنيها للصيرفة الإلكترونية الكثير من الوقت للعملاء للحصول على الخدمات الإلكترونية المختلفة وكذا المعلومات حول حساباتهم من مواقعهم البعيدة، خاصة في الأوقات الحرجة أو الضيقة.

9-مرونة عالية في الأداء: تمكنت المصارف حاليا من الابتكار في تقديم منتجاتها وخدماتها للعملاء نتيجة استفادتها من التكنولوجيا الحديثة حيث جعلت الصيرفة الإلكترونية من السهل على العملاء المقارنة والمفاضلة، فقد أخذت طابعا افتراضيا مع انعدام المعاملات الورقية، وعدم التقاء طالب الخدمة مع مقدمها ما جعلها أكثر مرونة.[1]

10-المحافظة على الموقع التنافسي والحصة السوقية للبنك: من خلال ارضاء جميع العملاء وتلبية حاجاتهم بسرعة أكبر وبطريقة مميزة فالبنك يحافظ على حصته السوقية وموقعه التنافسي.[2]

المطلب الثالث: متطلبات نجاح الخدمات الإلكترونية المصرفية

تُعد الثقة من العناصر الحساسة الهامة في بيئة الأعمال المصرفية بشكل عام، وفي الخدمات الإلكترونية المصرفية بشكل خاص، وتأتي هاته الأهمية من خلال تعزيز الثقة لدى العملاء لتُساهم في كسب ودَهم وجذبهم

[1] أحمد بوراس، السعيد بريكة، **نفس المرجع السابق**، ص 131.

[2] محمد علي خليل السميرات، **العوامل المؤثرة في استخدام الخدمات البنكية الإلكترونية عبر الهاتف المحمول من وجهة نظر العملاء: دراسة ميدان إقليم الجنوب–الأردن**، مجلة جامعة الشارقة للعلوم الإنسانية والاجتماعية، المجلد 14، العدد 1، 2017، ص 195.

من أجل التعامل مع البنك، لكن هاته الأخيرة لا تتأتى إلا بنجاح الخدمات الإلكترونية المصرفية، ولمعرفة سر هذا النجاح يجب توفر مجموعة من المتطلبات، وهذا ما سنتطرق إليه في هذا المطلب:

1-البنية التحتية الرقمية: إن من أهم مستلزمات أي مشروع تقني عموما، والصيرفة الإلكترونية خصوصا هي البنية التحتية التقنية، والبنى التحتية التقنية لا يمكن أن تكون معزولة عن بنى الاتصالات وتقنيات المعلومة التحتية للدولة ومختلف القطاعات، ذلك أن البنوك الإلكترونية هي تعيش في بيئة الأعمال الإلكترونية والتجارة الإلكترونية، والمتطلب الرئيسي لضمان أعمال إلكترونية ناجحة ودخول آمن وسلس لعصر المعلومات، يتمثل بالاتصالات، حيث أن كفاءة البنى التحتية وسلامة سياسات السوق الاتصالي، وتحديدا السياسات التسعيرية مقابل خدمات الربط بالإنترنت تلعب دورا هاما في اتساع نطاق العمل الإلكتروني، فلا تحيا الشبكات وأعمالها دون تزايد أعداد المشتركين الذين يعوقهم الوطن العربي تحديدا بكُلفة الاتصالات، والتي وإن كانت قد شهدت تخفيضا في بعض الدول العربية

لكنها ليست كذلك جميعا، وهاته المسألة تمثل أهم تحد أمام اعتماد الصيرفة الإلكترونية وتتطلب تدخلا جماعيا لرفع كل القيود التي تعترض تزايد استخدام الشبكة.[1]

والعنصر الثاني للبناء التحتي يتمثل بتقنية المعلومات، من حيث الأجهزة والبرمجيات والحلول والكفاءات البشرية المدربة والوظائف الاحترافي، وهاته دعامة الوجود والاستمرارية والمنافسة، ولم تعُد الأموال وحدها المتطلب الرئيسي، بل استراتيجيات التواؤم مع المتطلبات وسلامة البرامج والنظم المطبقة لضمان تعميم التقنية بصورة منظمة وفاعلة وضمان الاستخدام الأمثل والسليم لوسائل التقنية،[2] ولتغطية هذا العنصر على البنوك مراعاة عدة نقاط أهمها:

-توفير البرامج اللازمة للعمل المصرفي الإلكتروني: يجب على البنك امتلاك برامج جاهزة بدلا من تطويرها داخل البنك، لأن العمل المصرفي الحديث لا يتطلب بالضرورة سعي البنوك لتطوير برامج الحاسوب الداخلية، بل يمكنه الاعتماد على شركات متخصصة في هذا الميدان لتأمين احتياجاتها من تطبيقات البرامج لأغراض الأعمال الداخلية ولأغراض توزيع الخدمات المصرفية، وتؤكد التجارة العالمية أن شراء البرامج الجاهزة هو الأكثر فاعلية لامتلاك البرامج خاصة فيما يتعلق بفترة التسليم والتكلفة، وينبغي التأكيد هنا على أن الميزة التنافسية للبنك لا تكمن في تطوير برامجه الداخلية بل في توفير الخدمات وفق متطلبات العمل المصرفي الحديث.

-ضرورة امتلاك القدرة على اختيار الأجهزة المناسبة وإتاحة الفرصة أمام البنك لاختيار الشركة المصنعة للأجهزة، مع عدم الوقوع تحت رحمة شركة واحدة فقط، والاختيار معناه أيضا المنافسة بين الشركات المصنعة للأجهزة مما ينعكس إيجابيا على البنك خاصة على مستوى السعر ونوعية الخدمات وعصرنة التكنولوجيا.

---

[1] نادية شبانة، السعيد بريكة، **البنوك الإلكترونية الواقع والأفق**، دار الكتاب الحديث، القاهرة، مصر، الطبعة الأولى، 2016، ص 73.

[2] نور الدين بربار، محمد هشام قلمين، **نفس المرجع السابق**، ص 13.

– ضرورة مراعاة الاختلاف بين رجال البنك ورجال التكنولوجيا، حيث أن التكنولوجيا هي عنصر يساعد البنوك على تنفيذ أعمالها بكل كفاءة وفاعلية وتعزيز ربحيتها العامة، ولذا فإن الاتفاق على التكنولوجيا التي يجب اعتمادها يكون من قبل مديري البنوك وليس من قبل المسؤولين عن التكنولوجيا في البنك، فالتجارب العالمية تتضمن الكثير من الحالات التي تم فيها صرف مبالغ كبيرة على مشاريع تكنولوجية، والتي نتج عنها تكاليف ضخمة وتأخر في التوزيع بحيث أدت في أحيان كثيرة إلى التخلي عن المشروع ككل.

–ضرورة تغيير ثقافة موظفي البنك في اتجاهات التسويق والبيع وخدمة العملاء، حيث أن قبول العملاء لهذا التغيير في آليات توزيع الخدمة الجديدة يشكل شرطا أساسيا وحيويا لنجاح استثمار البنك في التكنولوجيا، وهذا لأمر صعب ويحتاج لفترة طويلة وتكاليف كبيرة لأنه يتعلق بتغيير العادات السلوكية للأفراد.

–أما عن عناصر إستراتيجية البناء التحتي في حقل الاتصالات وتقنية المعلومات، فتتمثل أساسا بتحديد أولويات وأغراض تطوير سوق الاتصالات في الدولة، مواجهة هدف الدخول للأسواق العالمية مع احتياجات تطوير التقنية للشركات الخاصة، سياسات تسويقية خدمية التنظيمية يتعين اعتمادها لضمان المنافسة في سوق الاتصالات، جذب الاستثمارات في هذا القطاع، تنظيم الالتزامات لمقدمي الخدمات مع تحديد معايير ومواصفات الخدمة المميزة في مقدمتها معايير أمن وسلامة تبادل المعلومات وسريتها وخصوصية المتعاملين.[1]

2–البنية القانونية: هي بمثابة الإطار التشريعي لأي عمل وإعطائه الدوافع والآثار المرجوة منه، وهاته القواعد تمثل الضمانة التي تحمي حقوق جميع المتعاملين في أي عمل شرعي، ولا شك أن العمليات المصرفية الإلكترونية هي تحتاج إلى بيئة قانونية تُثبتها وتعطيها مفعولها وتُكرس حقوق وواجبات كل طرف، سواء المؤسسات المصرفية أو العملاء.

حيث أصدرت اللجنة الاقتصادية والاجتماعية في الاتحاد الأوروبي سنة 1997 وثيقة بعنوان "المبادرة الأوروبية في التجارة الإلكترونية"، ومن بين المواضيع التي اهتمت بها هاته المبادرة الأوروبية هي ضرورة اعتماد نظام قانوني لمقدمي الخدمات الإلكترونية في السوق الأوروبية وحماية النظم الإلكترونية مثل التوقيع الإلكتروني والوثائق الإلكترونية ووسائل الدفع الإلكتروني. وتوفر البنى التحتية العامة يبقى غير كاف دون مشاريع بناء تحتية خاصة بالمنشآت المصرفية، وهو اتجاه تعمل عليه البنوك بجدية، وبناء على ذلك فإن عنصر التميز هو إدراك مستقبل تطور التقنية وتوفير بُنى وحلول برمجية تُتيح مواصلة التعامل مع المستجدات، فتقنية حصرية تعني أداءً ضيقا والمسألة ليست مسألة أموال إنما خُطط سليمة وكفاءات إدارية مميزة ترى المستقبل أكثر مما ترى الحاضر ولا تتباهى بما تنجزه بقدر ما تشعر بثقل مسؤولية البقاء ضمن المميزين.[2]

3–التطوير والاستمرارية والتفاعلية مع المستجدات: يُقدم عنصر التطوير والاستمرارية والتنويع على العديد من

[1] بن صالح ماجدة، **نفس المرجع السابق**، ص 96.

[2] يوسف حسن يوسف، **البنوك الإلكترونية**، المركز القومي للإصدارات القانونية، القاهرة، مصر، الطبعة الأولى، 2012، ص 68.

عناصر متطلبات الصيرفة الإلكترونية، فالجمود وانتظار الآخرين لا يتفق مع التقاط فُرص التميز، فالبنوك العربية مثلا-لا تتجه دائما نحو الريادة في اقتحام الجديد، إنما تنتظر أداء الآخرين، وربما يكون المبرر لذلك هو الخوف على أموال المساهمين واجتياز المخاطر، وهو أمر مهم وضروري لكنه ليس مانعا من الريادية، والريادية في نفس الوقت لا تعني اقتحام الجديد والتسرع في التخطيط للتعامل مع الجديد وإعداد العدة، لكنها حتما تتطلب السرعة في إنجاز ذلك.[1]

4-كفاءة الأداء المتفقة مع عنصر التقنية: تقوم هاته الكفاءة على فهم احتياجات الأداء والتواصل التأهيلي التدريبي، والأهم من ذلك أن تمد كفاءة الأداء إلى كفاءة الوظائف الفنية والمالية والتسويقية والقانونية والاستثمارية والإدارية المتصلة بالنشاط المصرفي الإلكتروني والكفاءات البشرية المدربة والوظائف الاحترافية.

5-التفاعل مع متغيرات الوسائل والاستراتيجيات الفنية والإدارية والمالية: إن التفاعلية لا تكون في التعامل مع الجديد فقط أو مع البنى التكنولوجية فقط، وإنما مع الأفكار والنظريات الحديثة في حقول الأداء الفني والتسويقي والمالي والخدمي، تلك الأفكار التي هي وليدة تفكير إبداعي وليست وليدة تفكير نمطي.

6-الرقابة التقييمية الحيادية: من أهم عناصر النجاح هو اعتماد جهات رقابية واستشارية قادرة على التقييم الموضوعي، ومن هنا أقامت غالبية البنوك التي اعتمدت على الصيرفة الإلكترونية جهات استشارية في التخصصات التقنية والقانون والنشر الإلكتروني والتسويق لتقييم فعالية وأداء مواقعها، حيث أن عدد زائري الموقع ليس وحده مؤشرا على النجاح، إذ يسود فهم عام أن كثرة زيارة الموقع على محركات البحث وسلامة الخُطط الدعائية والترويجية.[2]

المطلب الرابع: نظام الدفع في الخدمات الإلكترونية المصرفية

إن أنظمة الدفع الإلكتروني في الخدمات الإلكترونية المصرفية تُعتبر من الضمانات الأساسية واللازمة لنموها واستمراريتها وتطوير أدائها، كما أنها تطورت بشكل كبير وواسع في الآونة الأخيرة، ولغرض تقييم كفاءة أداء العمل المصرفي في فترة معينة، فإن ذلك يعني ضرورة استخدام وسائل الدفع الإلكترونية ومواكبة التكنولوجيا لتحديد الأهداف التي تضمن للمصرف وصوله إلى تحقيق غايته في الربحية المنشودة.

حيث يمكن تعريف نظام الدفع الالكتروني Payement Gateway على أنه وسيلة لربط التاجر بالزبون بشكل إلكتروني، إذ يستطيع الزبون الذي يمتلك بطاقة الدفع الإلكترونية أن يقوم بالشراء من التاجر الذي يمتلك موقع تجاري على الإنترنت، ويكون المصرف هنا وسيطا بينهما، إذ يُحوَل من رصيد الزبون إلى رصيد التاجر، وهذا ما يُشكل نظام الدفع الإلكتروني.

---

[1] السعيد بريكة، نادية شبانة، **المرجع السابق نفسه**، 2016، ص 75.

[2] عامر إبراهيم قنديلجي، **التجارة الإلكترونية وتطبيقاتها**، دار الميسرة للنشر والتوزيع والطباعة، عمان، الأردن، الطبعة الرابعة، 2015، ص 177.

فالدفع الإلكتروني هو خدمة مصرفية يقدمها المصرف لزبائنه بحيث يستطيعون أن يُسددوا ما عليهم من التزامات (فواتير، رسوم، ضرائب،...إلخ)، وكما يستطيعون أن يشتروا برامج وألعاب وأفلام وتطبيقات وأغراض أخرى، أو يقومون بتوصية على البضائع عن طريق موقع الشركات الصناعية بأنواعها المختلفة وهم في بيوتهم، لهذا فإن نظام الدفع الإلكتروني يمثل العمود الفقري للتجارة الإلكترونية.[1]

اعتُبر الدفع الإلكتروني أنه: "عملية تحويل الأموال في الأساس ثمن لسلعة أو خدمة باستخدام أجهزة الكومبيوتر وارسال البيانات عبر خط تليفوني أو شبكة ما، أو أي طريقة كانت لإرسال البيانات".[2]

وفي الجزائر، عرَف المشرِع الدفع الإلكتروني في القانون المتعلق بالتجارة الإلكترونية رقم: 05-18، المؤرخ في: 10 ماي 2018، في المادة رقم: 06 الفقرة 05 التي نصَت بأنه: "كل وسيلة دفع مرخَص بها طبقا للتشريع المعمول به تُمكن صاحبها من القيام بالدفع عن قُرب أو عن بُعد، عبر منظومة إلكترونية".[3]

ومن خلال ما سبق يتضح لنا أن نظام الدفع الإلكتروني أحدث تغيرا جذريا في نمط العمل المصرفي، إذ عرف انتشارا واسعا في الآونة الأخيرة، وأصبح من بين أهم الخدمات التي تُتيحها البنوك لعملائها لإجراء عمليات البيع والشراء من خلال شبكة الإنترنت، وكذا الاستفادة من الخدمات الإلكترونية المصرفية المختلفة.

وبالنسبة لتجربة الجزائر في الصيرفة الإلكترونية وأنظمة الدفع في خدماتها، شهدت دخولا متأخرا ليس مقارنة بدول أمريكا الشمالية وآسيا وأوروبا فقط وإنما أيضا مقارنة مع الدول النامية ودول الشرق الأوسط وشمال إفريقيا التي تتساوى معا في العديد من مؤشرات النمو والتنمية الاقتصادية والاجتماعية.[4]

في السنوات الأخيرة شهدت أنظمة الدفع الإلكترونية عبر شبكة الإنترنت بمختلف أنواعها في الجزائر تطورا ملحوظا، وهذا مؤشر جد مهم، فمنذ شهر أكتوبر لسنة 2016، أصبح الدفع الإلكتروني عن طريق الإنترنت بواسطة البطاقات المصرفية المختلفة عملًيا بالجزائر، حيث تم فتح هاته الخدمة في المرحلة الأولى للقائمين على الفوترة ذات المبالغ المالية الكبيرة مثل: شركات توزيع الماء والطاقة، الكهرباء والغاز (سونلغاز)، الهاتف الثابت والنقال، شركات التأمين، النقل الجوي وبعض الإدارات، فحاليا يوجد **370** تاجر الويب منخرط في نظام الدفع الإلكتروني المصرفي، منذ انطلاق الدفع الإلكتروني، نتج عنه حوالي: **32.246.627** معاملة إلكترونية إلى غاية شهر جوان من سنة 2023، موزعة يمكن ملاحظتها من خلال الجدول التالي:

---

[1] حسين القاضي، مادلين عبود، سمى سنكري، **واقع تقنيات الدفع الإلكتروني في المصارف السورية**، مجلة جامعة ترشين للبحوث والدراسات العلمية، سوريا، العدد 5، 2012، ص 247.

[2] مصفح فاطمة، آيت علي زينة، **مفهوم الدفع الإلكتروني وتمييزه عن الدفع التقليدي**، مجلة البحوث والدراسات القانونية والسياسية، المجلد 11، العدد 02، 2022، ص 224.

[3] قانون رقم: 05-18، **المتعلق بالتجارة الإلكترونية**، المؤرخ في: 10 ماي 2018، ج ر ج ج، العدد 28، الصادر في 16 ماي 2018.

[4] عبد الرحيم بلبالي، **واقع الصرفة الإلكترونية في الجزائر وآليات تفعيلها**، المجلة المتوسطية للقانون والاقتصاد، 2019، ص 202.

الجدول رقم (II–2): توزيع نشاط الدفع بالبطاقات الإلكترونية المصرفية بالجزائر

السنة	هاتف اتصالات	نقل	تأمين	فاتورات كهرباء–ماء	خدمة إدارية	خدمات	بيع سلع	رياضة وترفيه
2016	6536	388	51	391	0	0	0	0
2017	87286	5677	2467	12414	0	0	0	0
2018	138495	871	6493	29722	1455	0	0	0
2019	141552	6292	8342	38806	2432	5056	0	0
2020	4210284	11350	4845	85676	68395	213175	235	0
2021	6993135	72164	8372	120841	155640	457726	13468	0
2022	7490626	195490	23571	302273	153957	705114	24163	152925
إلى جوان 2023	4128658	147906	15844	281450	4522	444051	21109	464679

المصدر: https://giemonetique.dz/ar، **تاريخ الاطلاع: 19–08–2023، الساعة: 16:00.**

بقراءتنا للجدول أعلاه نلاحظ أنه نتج عن تلك المعاملات الإلكترونية المختلفة عدد معتبر من عمليات الدفع الإلكتروني بمبالغ إجمالية معتبرة، ويمكن ملاحظتها في الجدول أدناه، موزعة بالترتيب عبر السنوات التالية:

الجدول رقم (II–3): إجمالي نشاط الدفع بالبطاقات الإلكترونية المصرفية بالجزائر

السنة	عدد معاملات الدفع	المبلغ الإجمالي لمعاملات الدفع
2016	7366	15009842.02دج
2017	107844	267993423.40دج
2018	176982	332592583.28دج
2019	202480	503870631.61دج
2020	4593960	5423727074.80دج
2021	7821346	11176475535.68دج
2022	9048125	18151104423.96دج
إلى غاية جوان 2023	899829	8729764118.33دج

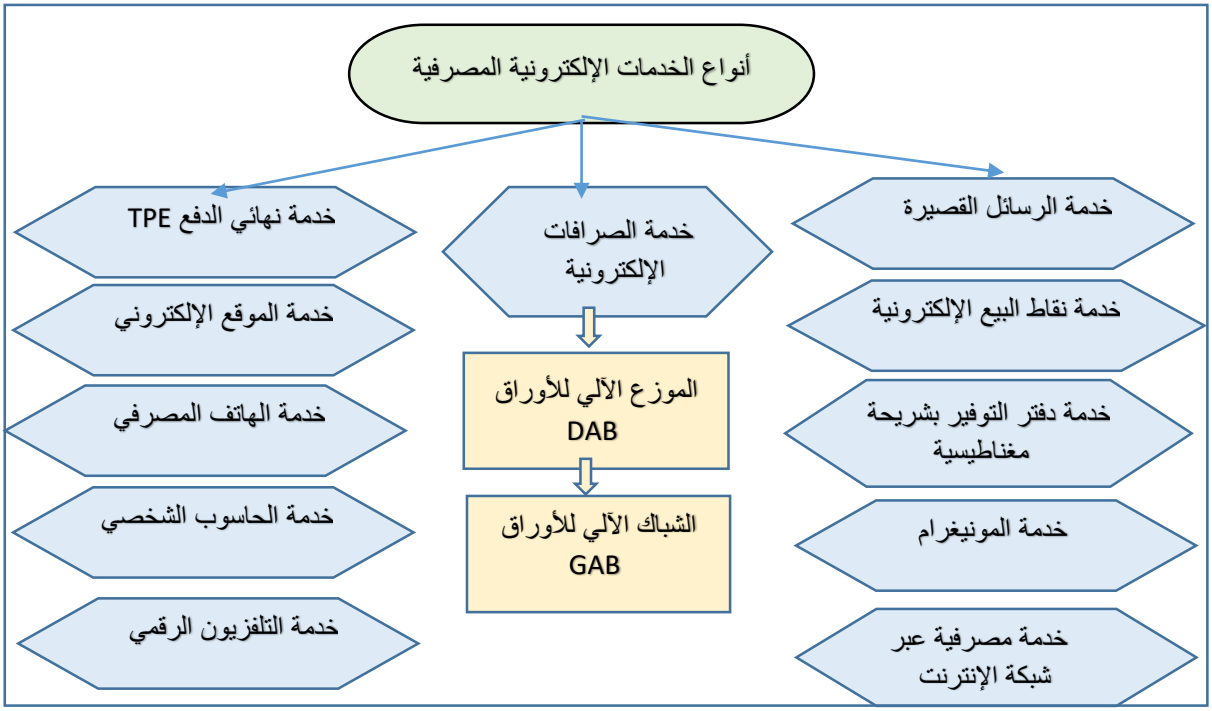
المصدر: https://giemonetique.dz/ar، **تاريخ الاطلاع: 19–08–2023، الساعة: 16:00.**

من خلال ما تضمنه الجدولين المذكورين أعلاه رقم: (II-2)، ورقم: (II-3)، يتضح لنا جليا تطور نسبة استخدام بطاقات الدفع الإلكترونية المصرفية من خلال أجهزة الدفع الإلكترونية TPE وأجهزة الصراف الآلي ATM، حيث تطور حجم المعاملات المالية المختلفة عبر شبكة الإنترنت، ما بين الفترة: 2016 إلى غاية شهر جوان 2023، كما نلاحظ زيادة مستمرة في عدد الخدمات الإلكترونية، فشهدت بداية: 2020-2021 تطورا ملحوظا ونموا إيجابيا في عدد معاملات الدفع الإلكتروني عبر شبكة الإنترنت وكذا المبلغ الإجمالي لها، يمكن تفسير سبب ذلك إلى السياسة المتبعة من قبل الدولة ونمو ثقافة المجتمع الجزائري، ورغم ذلك لا يزال بعيدا عن المستوى المطلوب مقارنة ببعض الدول النامية دون الحديث عن دول العالم المتقدم، وما يمكن أن يزيد في تفسير هذا النمو، جائحة كورونا التي عززت مثل هاته المعاملات الإلكترونية بسبب تجنب تلاقي العنصر البشري وجها لوجه خوفا من تنقل عدوى المرض، ضف إلى ذلك تكسُر حاجز عدم الثقة والخوف من استخدام الخدمات الإلكترونية المصرفية.

المطلب الخامس: أنواع الخدمات الإلكترونية المصرفية

تسعى مختلف البنوك إلى تقديم خدمات إلكترونية مصرفية متنوعة تتماشى وحاجات عملائها، من خلال مواكبة التقنية الحديثة، ما أدى إلى رفع مستوى الخدمة وجودتها والارتقاء بها، وكذلك الحصول على درجة عالية من رضا وثقة العملاء، وفيما يلي سيتم عرض أنواع الخدمات الإلكترونية المصرفية في شكل مُبسط ومُختصر.

الشكل رقم (II-1): أنواع الخدمات الإلكترونية المصرفية



المصدر: من اعداد الطالب بالاعتماد على أنواع الخدمات الإلكترونية المصرفية.

من خلال الشكل أعلاه، سنتطرق بعرض وشرح كل نوع من أنواع الخدمات الإلكترونية المصرفية، حتى تكون لدينا معرفة شاملة لها:

- **خدمات الصيرفة الإلكترونية من خلال الصراف الآلي (ATM): Automatic Teller Machine**

✓ **الصراف الآلي:** هو جهاز إلكتروني مهمته القيام ببعض الأعمال الإلكترونية مثل حفظ النقود بطريقة آلية، وبكمية مُحددة من العملات لتسهيل عملية إجراء السحب النقدي من قبل العملاء، كما يحمل الجهاز رقم سري يُمكّن العميل من الحصول على بعض الخدمات الإلكترونية المصرفية مثل طلب دفتر الشيكات وذلك بهدف تقليل الجهد والحصول على هذه الخدمات حتى في غير أوقات العمل الرسمية.

الشكل رقم (II-2): الصراف الآلي (ATM)

المصدر: www.bdl.dz بتاريخ: 2023.08.20، الساعة: 09:00.

هي أكثر الخدمات الإلكترونية انتشارا، فالماكينة مُبرمجة تُحفظ فيها النقود وتستطيع التعرف على البطاقات المغناطيسية الخاصة بها، تُوفرها البنوك في معظم فروعها بهدف تخفيف ضغط العمل وتجنب الإجراءات الإدارية وتلبية حاجات العملاء المالية بعد أوقات العمل وخلال العطل، وتُعد هذه الأجهزة من أهم أنماط الصيرفة الإلكترونية التي تؤدي دورا هاما في توزيع المنتجات المصرفية، وذلك من خلال:

✓ **الموزع الآلي للأوراق (DAB) Distributeurs Automatique de Billets**

هو آلة أوتوماتيكية تسمح للعملاء عن طريق بطاقاتهم الإلكترونية بسحب مبالغ من المال دون الحاجة للُجوء إلى فروع البنك وهذا على مدار 24/24سا وخلال كل أيام الأسبوع، والجدول التالي يشرح طريقة عمل الموزع الآلي للأوراق مع النتائج والمبادئ العامة له.

الجدول رقم (II–4): الموزع الآلي للأوراق (DAB)

	المبادئ العامة	التقنية	النتائج
الموزع الآلي للأوراق DAB	-يسمح بالسحب لكل عميل يحوز على بطاقة السحب الإلكترونية. -يوجد في البنوك، الشوارع، أماكن أخرى. -يعمل باستمرار ودون انقطاع.	-جهاز موصول بوحدة مراقبة إلكترونية مبرمجة كي تقرأ المدارات المغناطيسية للبطاقة الإلكترونية، هذه الأخيرة نسجل عليها المبالغ المالية الممكن سحبها في أي وقت.	-تخفيض نشاط السحب في الفروع.

المصدر: مصطفى كافي، النقود والبنوك الإلكترونية، دار مؤسسة راسلان للطباعة والنشر والتوزيع دمشق، سوريا، 2011، ص 157.

الشكل رقم (II–3): الموزع الآلي للأوراق (DAB)

المصدر: www.bdl.dz أطلع عليه بتاريخ: 2023.08.19، الساعة: 09:20.

✓ الشباك الآلي للأوراق Guichet Automatique de Bancaire (GAB):

الشبابيك الأوتوماتيكية للأوراق هي عبارة عن أجهزة أوتوماتيكية متصلة بالحاسوب الرئيسي للبنك، تقدم خدمات أكثرا تعقيدا وأكثر تنوعا بالنسبة للموزع الآلي للأوراق عن طريق بطاقات إلكترونية، وبالإضافة إلى خدمة السحب النقدي تسمح بالقيام بالعديد من العمليات من 12 إلى 15 عملية في البنوك الفرنسية ومن 65 إلى 75 عملية في البنوك الأمريكية.

هذه الخدمات تشمل مثلا: عمليات التحويل من حساب إلى حساب آخر، قبول الودائع، طلب الصكوك، ....إلخ، وهي تُمثل في الوقت الحاضر أحد المنتجات البنكية الإلكترونية الأساسية للنظام البنكي، ودورها مُهم على مستوى التسويق لأنها أصبحت تمثل وسيلة للحوار مع المستهلك، الاستفسار عن أسعار العمولات، جهاز بيع وشراء العملات الأجنبية بشكل آلي.[1]

والجدير بالذكر أنه مع تطور عمل الصرافات الآلية أصبحت تقوم حاليا بدفع الفواتير للمؤسسات الخدمية المختلفة، كتسديد الرسوم الحكومية وذلك بواسطة نظام التبادل الإلكتروني للبيانات، وهو نظام يسمح بنقل رسائل الكمبيوتر لجهاز كمبيوتر آخر.

الشكل رقم (II-4): الموزع الآلي (GAB)

المصدر: www.bdl.dz بتاريخ: 2023.08.19، الساعة: 10:00.

ويتميز نظام خدمة الصراف الآلي بما يلي:[2]

-سرعة المعاملات، حيث لا يستطيع العميل التعامل مع النظام إلا من خلال الرقم السري الخاص به.

-سهولة وسرعة التعامل مع الآلة أفضل حل لمشاكل الازدحام والانتظار.

-إمكانية تحويل المبالغ من حسابات العميل المسموح التعامل عليها من خلال النظام.

-إمكانية سداد الالتزامات المالية الشهرية والنصف سنوية.

[1] ياسع ياسمينة، تومي عبد الرحمان، **دراسة تحليلية لتطور نشاط الصيرفة الإلكترونية في الجزائر من خلال أهم المؤشرات-تحليل مقارن**، "مداخلة مقدمة ضمن فعاليات الملتقى الوطني الثامن حول آليات تفعيل وسائل الدفع الحديثة في النظام المالي والمصرفي الجزائري"، تنظيم كلية العلوم الاقتصادية والتجارية وعلوم التسيير جامعة البويرة، الجزائر، يومي 14/13 مارس، 2017، ص 05.

[2] إبراهيم بختي، **محاضرات في مقياس الصيرفة الإلكترونية**، اختصاص مالية وبنوك، قسم العلوم الاقتصادية، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة قاصدي مرباح ورقلة، الجزائر، 2018، ص14.

➢ كما يوفر هذا النظام الخدمات التالية للعملاء:

-الاستفسار عن أرصدة حسابات العميل المسموح بالتعامل عليها من خلال النظام.

-السحب من أرصدة حسابات العميل المسموح بالتعامل عليها من خلال النظام.

-الإيداع النقدي وطلب دفتر الشيكات.

-السحب السريع ويُحدده البنك مُسبقا، ويكون بمبالغ صغير أو متوسطة.

-الاستفسار عن أسعار العملات.

والجدول التالي يلخص بعض العناصر السابقة لطريقة عمل الموزع الآلي بالإضافة إلى النتائج:

الجدول رقم (II-5): الموزع الآلي (GAB)

	المبادئ العامة	التقنية	النتائج
الموزع الآلي GAB	-يخول لكل حائز على البطاقة الإلكترونية القيام بالعديد من العمليات منها: السحب و معرفة الرصيد طلب شيكات القيام بتحويلات	-جهاز موصول بالكمبيوتر الرئيسي للبنك حيث يقرأ المدارات المغناطيسية للبطاقة هذه الأخيرة يسمح من خلالها بمعرف الرصيد بفضل الرمز السري.	-يستعمل من طرف العملاء في أوقات غلق البنوك، خاصة العميل المستعجل.

المصدر: مصطفى كافي، المرجع السبق ذكره، ص 158.

- **الخدمة الإلكترونية المصرفية عبر الهاتف "الهاتف المصرفي": Mobile Banking**

مع تطور الخدمات الإلكترونية المصرفية على مستوى العالم، أنشأت المصارف خدمة الهاتف المصرفي، وهي تتم من خلال التلفون المحمول من الأنواع التي تقدم تكنولوجيا الجافا (Java Technology)، وهي عبارة عن تطبيقات وبرمجيات موجودة في أجهزة الهاتف المحمول تعتمد على إقامة قناة اتصال مباشر بين المصرف والعميل عن طريق تقنية wap،[1] تسمح بتنفيذ العمليات المصرفية ضمن إجراءات إلكترونية، من خلال الاتصالات المتنقلة واستخدام أجهزة الهاتف المحمول، وذلك لتسهيل إدارة العملاء لعملياتهم المصرفية وتفادي طوابير الانتظار للاستفسار عن حساباتهم والاطلاع على الرصيد، وتستمر هذه الخدمة على مدار 24/24 ساعة بما في ذلك العطل والإجازات الرسمية، تُقدم هذه الخدمة بالاعتماد على شبكة الإنترنت المرتبطة بفروع المصرف، والشكل التالي سيوضحها:

[1] خالد سحنون، **تأثير تكنولوجيا المعلومات على مردودية البنوك**، أطروحة مقدمة لنيل شهادة الدكتوراه، تخصص علوم اقتصادية، جامعة أبو بكر بلقايد، تلمسان، الجزائر، 2016، ص 174.

الشكل رقم (II–5): الهاتف المصرفي

المصدر: www.bdl.dz بتاريخ: 2023.08.20، الساعة: 10:40.

وهذه الوسيلة تمكن العملاء من الحصول على خدمات محددة فقط بإدخال الرقم السري الخاص، وما على المصرف سوى التأكد من هوية العميل، وقد تعددت الخدمات التي يقدمها الهاتف المصرفي للعملاء على مستوى العالم، ومن بين هذه الخدمات، التحويل ما بين الحسابات الشخصية، الاستعلام عن الأرصدة للحسابات الشخصية، التحويل من حساب عميل إلى حساب عميل آخر، وكذا إمكانية العملاء بشراء سلعة أو خدمة وإضافة حسابه على فاتورة هاتفه المحمول، بحيث تقوم شركة الاتصالات التي يتعامل معها بالدفع، ثم تقوم شركة الاتصالات بإضافة هذا المبلغ إلى فاتورة العميل، إضافة لباقة من الخدمات الأخرى التي تنفرد بها مصارف عن أخرى، وفي أمريكا بدأت هذه الخدمة مع بنك "ميدلاند" الذي يقوم بتوفيرها تحت اسم الحساب الأول المباشر عن طريق الاتصالات الهاتفية بإدخال الرقم السري الخاص بالعميل، وهذا ما يمكنه من تحويل الأموال أو الأمر بالدفع لصالح دائنه، كسداد بعض التزاماته مثل فاتورة الهاتف، الكهرباء، الغاز.

أما في بريطانيا أدخلت هذه الخدمة منذ سنة 1985 وكانت تعمل بواسطة شاشة لدى العميل في منزله لها اتصال مباشر، تمكنه من معرفة كل المعلومات التي هو في حاجة إليها، وفي سنة 1986 تم إدخال خدمات جديدة للهاتف المصرفي تتمثل في خدمة التحويلات المالية من حساب العميل المدفوعة عليه لسداد كمبيالات والفواتير، أما سنة 1987 تمت إضافة خدمة الصوت أي محادثة العميل والمصرف مباشرة من خلال الحساب الآلي الخاص بالعميل، وفي سنة 1994 تم استحداث "باركليز بنك" خدمة تحويل الأموال ودفع الالتزامات، وأتاحت خدمة الهاتف المصرفي للعميل فرصة التعاقد للحصول على قرض أو فتح اعتمادات مستندية وغيرها.

وتُعتبر ألمانيا أول دولة تقوم بإدخال خدمة الهاتف المحمول في العالم، حيث قدم أحد البنوك الألمانية في أول جانفي لسنة 2000 خدمة البنك المحمول، ليحقق لعملائه الاتصال من خلال الهاتف المحمول بالبنك

عن طريق موقع (Yahoo) على الإنترنت من أي مكان، وقد بدأت العديد من البنوك العالمية في إدخال هذه الخدمة، وبصفة عامة تتفوق أوروبا على و.م.أ في تقديم الخدمات المصرفية المتنوعة عبر المحمول.[1]

بالنسبة لبنك التنمية المحلية BDL من خلال الهاتف المحمول تسمح لك بتحميل تطبيق Mobile BDL على متجر Play Store أو Apple Store للاستفادة من "**خدمة ديجيت بنك**": هاته الخدمة تسمح لزبائن البنك بالاطلاع على حساباتهم البنكية في أي وقت، مع القيام بعمليات الدفع العادية، وتحميل الرصيد، وطلب دفتر الشيكات، والتحويل من حساب لآخر.[2]

- **خدمة الرسائل القصيرة SMS (الصيرفة عن طريق SMS):**

هي تقنية جديدة تسمح للعميل بمتابعة كافة العمليات المصرفية الخاصة به، أو التي تمت على حسابه الشخصي أولاً بأول من خلال استلامه رسالة نصية تلقائية من البنك على هاتفه النقال تُخبره بحدوث حركات أو عمليات معينة، ومن أهم الرسائل القصيرة: رسالة رصيد الحساب، رسالة وصول الراتب، رسالة وصول حوالة، رسالة الإيداع النقدي، رسالة السحب النقدي، رسالة التحويلات بين الحسابات...الخ.

الشكل رقم (II–6): الخدمة المصرفية عن طريق SMS

المصدر: www.bdl.dz بتاريخ: 2023.08.20، الساعة: 11:05.

أصبحت الآن الخدمة المصرفية عن طريق SMS تُرسل للعميل أية حركة مالية على حسابه، وتخبره بأية خدمات مثل: استحقاق الوديعة، استحقاق كمبيالة، قروض أو كفالة...الخ الموافقة على القروض ومراجعة البنك لسبب ما.

[1] ياسمينة ياسع، تومي عبد الرحمان، **نفس المرجع السابق**، ص 4.

[2] هجيره ديدوش، حريزي عبد الغني، **واقع الخدمات المصرفية الإلكترونية بالبنوك الجزائرية، مجلة استراتيجيات التحقيقات الاقتصادية والمالية**، المجلد 04، العدد 01، 2022، ص 29.

- **خدمة نهائي الدفع (TPE) أو خدمة نقطة البيع: Point of sale service**

يتم استخدام جهاز للدفع الإلكتروني (TPE)* متصل بشبكة إلكترونية مع البنوك يتم فيه التحويل إلكترونيا للنقود من حساب العميل (المشتري) إلى حساب التاجر باستخدام البطاقة المصرفية، حيث يستخدمها العميل عند دفع قيمة الخدمات والسلع التي يحصل عليها لدى محلات التجارية والمطاعم وغيرها من المرافق التجارية.

الشكل رقم (II–7): نهائي الدفع الإلكترونية (TPE)

المصدر: www.bdl.dz بتاريخ: 2023.08.20، الساعة: 14:00.

تسمح هذه التقنية للزبون باستخدام بطاقات بلاستيكية أو بطاقات ذكية للقيام بأداء مدفوعات، من خلال الخصم على حسابه إلكترونيا إلى رصيد المتجر إلكترونيا بتمرير البطاقة الائتمانية على القارئ الإلكتروني الخاص ببطاقات الائتمان، والموصول مباشرة مع الحاسوب المركزي للبنك المعني بإدخال الرقم السري وبالتأكد من كفاية الرصيد.[1]

الجدول التالي يوضح باختصار طريقة عمل نهائي الدفع الإلكترونية ونتائج خدماته.

جدول رقم (II–6): نهائي الدفع الإلكترونية (TPE)

	المبادئ العامة	التقنية	النتائج
نهائي الدفع الإلكتروني TPE	-يوضع في المحلات حيث يسمح للعميل بتسوية عملياته التجارية المختلفة بالبطاقات الإلكترونية أثناء التسديد.	-فروع موصولة بشبكة تجمع عدة بنوك.	-يحل عدة مشاكل تخص نقل الأموال، ويوفر الأمان اللازم.

المصدر: مصطفى كافي، المرجع السبق ذكره، ص 159.

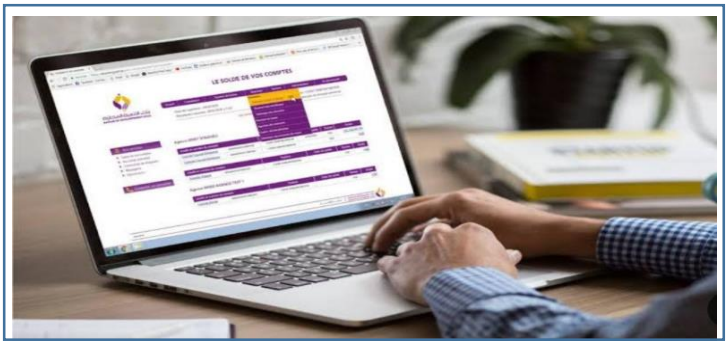
(*): (TPE) Terminal de Paiement Electronique

[1] محمد عبد حسين الطائي، "**التجارة الإلكترونية، المستقبل الواعد للأجيال القادمة** "، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2010، ص 232.

- **خدمات الحاسوب الشخصي، البنك المنزلي (Pc Banking):**

بدأت مجموع من المصارف العالمية الكبرى في تطبيق النظم المصرفية المباشرة مع العملاء من خلال الحاسب الآلي المتواجد في المنزل أو المكتب.

الشكل رقم (II–8): خدمات الحاسوب الشخصي (Pc Banking)



المصدر: www.bdl.dz بتاريخ: 2023.08.20، الساعة: 16:40.

تسمح هذه الخدمة للعملاء بالتعامل مع العديد من المعاملات المصرفية عبر جهاز الحاسوب الشخصي، وهذا بعد تحميله ببرنامج خاص، يوفره البنك مجانا أو مقابل رسوم خفيفة، للاطلاع على الحساب والتصرف (السحب والإيداع) في أرصدة الحسابات المصرفية، وكذا القيام بمقابلة على شاشة الحاسوب مع موظف المصرف، وهذا لتقديم النصائح المالية واستقبال الردود عن الأسئلة وغيرها، وكل هذا عن طريق خط خاص يبدأ طرفه من المكتب أو المنزل أو أي مكان آخر وفي أي وقت، وينتهي طرفه الثاني عند الحاسوب المركزي للبنك. وتطور هذا الأسلوب مع شيوع الإنترنت إذ أمكن للزبون الدخول وإجراء المعاملات من خلال الاتصال بالشبكة، لكن في ظل ضوابط تتحكم في حركة هذه الأنشطة لتضمن حقوق العملاء والبنك على حد سواء.

- **خدمات التلفزيون الرقمي:**

هي عبارة عن ربط الأقمار الصناعية بين جهاز التلفزيون بالمنزل وحساب المصرف، بحيث يمكن الدخول من خلال الرقم السري إلى حساب المصرف أو شبكة الإنترنت وتنفيذ العمليات المطلوبة.

الشكل رقم (II–9): التلفزيون الرقمي

المصدر: www.bdl.dz بتاريخ: 2023.08.20، الساعة: 20:15.

هذه الطريقة تسمح بالتفاعل السهل وخصوصا لربات البيوت ولاسيما في حال عدم توفر جهاز الإنترنت، يتم الانتفاع بخدمات التلفزيون الرقمي.

- **الخدمة المصرفية عبر شبكة الإنترنت: On–Banking line:**

تسمح هذه الخدمة للعملاء من خلال موقع البنك مثلا: (https://www.bdl.dz) على الإنترنت بالتعامل والاستعلام عن حساباتهم من أجهزتهم الشخصية في المنازل أو المتاجر أو المكاتب، وذلك بواسطة رقم سري خاص لكل منهم، إذ يمكن للعملاء التعامل بالمعلومات الخاصة بهم وبالتالي يمكن التحكم في أموالهم مع توفر إجراءات الحماية والأمان في عملية التصفح والبحث وكذلك طباعة أية معاملة.

الشكل رقم (II–10): قناة إجراء العمليات المصرفية

المصدر: www.bdl.dz بتاريخ: 2023.08.20، الساعة: 21:50.

يُطلق أحيانا مصطلح بنوك الإنترنت على عمليات الصيرفة عبر الحاسوب الشخصي، حيث تستخدم الإنترنت الموقع الإلكتروني كقناة لتسليم منتجات وخدمات هذه الأخيرة، ولقد ساهم استخدام الإنترنت في تقديم هذه الخدمة ومن ثم قامت أغلب المصارف بإنشاء مواقع لها عبر شبكة الإنترنت بدلا من انشاء مقرات جديدة، حتى يستطيع العميل أن يتصل بالفرع الإلكتروني بطريقة أسهل ويعرض المصرف على الإنترنت مجموعة من الخدمات أهمها ما يلي:[1]

- ✓ دفع الفواتير.
- ✓ النشرات الإعلامية عن الخدمات المصرفية.
- ✓ إجراء تحويلات الأموال بين حسابات العملاء.
- ✓ عرض وتدقيق أرصدة حساب التوفير.
- ✓ دفع قيم الرهون العقارية.

[1] أحمد بوراس، السعيد بريكة، **نفس المرجع السبق**، ص99.

ويرى المحللون أن الإنترنت وسيلة لزيادة القطاعية السوقية وآلية جذب فهي تزيد من عدد العملاء باستمرار، حيث جعلت من السهل وضع قاعدة جديدة من العملاء والاستحواذ على حصة أكبر من موجودات المودع، إذ يحتاج هذا النوع من الخدمة إلى توفير شبكات عريضة داخل البلاد على الأقل وربطها بالشبكة العالمية للإنترنت، وتتطلب من العميل استخدام برامج التصفح على الشبكة، الشيء الذي يلقى على عاتق البنوك مهمة عرض وتنسيق بياناتها على شبكة الإنترنت، وذلك بخفض التكلفة واقتناع العملاء بأن الصيرفة عبر الموقع الإلكتروني (عبر الإنترنت) وسيلة آمنة.

- **خدمات نقاط البيع الإلكترونية:**

هي الآلات التي تنتشر لدى المؤسسات التجارية والخدمية بمختلف أنواعها وأنشطتها، ويمكن للعميل استخدام بطاقات بلاستيكية أو بطاقات ذكية للقيام بأداء المدفوعات من خلال الخصم على حسابه إلكترونيا بتمرير هذه البطاقة داخل هذه الآلات المتصلة إلكترونيا بحاسب المصرف.

الشكل رقم (II-11): خدمات آلات الدفع في المحلات التجارية والخدمية مع البطاقات الذكية

المصدر: www.bdl.dz بتاريخ: 2023.08.20، الساعة: 23:10.

من بين الخدمات المالية التي تقدمها هذه الأخيرة:[1]

- ✓ الدفع الآلي في المحلات التجارية.
- ✓ ضمان الشيكات.
- ✓ القيد المباشر عن طريق التحويل الإلكتروني من حساب المشتري إلى حساب التاجر باستخدام جهاز(EPOS).

[1] صلاح الدين حسن السيسي، **التجارة الدولية والصيرفة الإلكترونية، النظريات والسياسات**، دار الكتاب الحديث، القاهر، مصر، 2014، ص 129.

- **خدمة دفتر التوفير بشريحة مغناطيسية:**

يُعتبر الادخار والاستعمال الواسع النطاق للدفتر المعالج بالطرق المعلوماتية جزء من برنامج التحديث للبنك، حيث أن وجود شريط مغناطيسي على الكتيب الجديد لدفتر التوفير يجعله سهلا للاسخدام، ويمكن عملاء البنك بالقيام بعمليات السحب والدفع الفوري والاطلاع على الرصيد، كما يمكن من خلاله تسليم نسخ تأكيد القيام بالعمليات.

الشكل رقم (II–12): دفتر التوفير بشريحة مغناطيسية

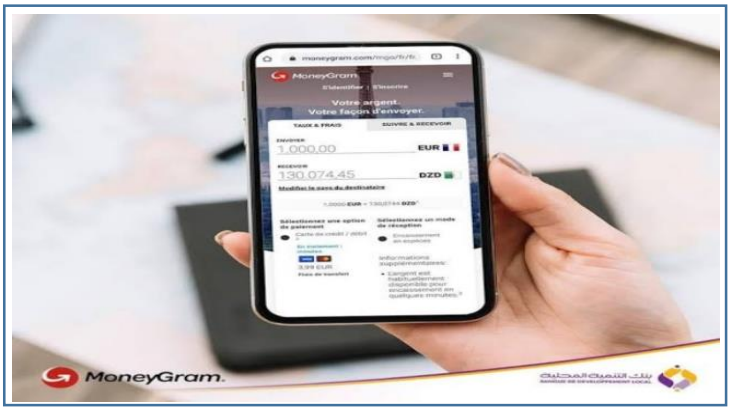
المصدر: www.bdl.dz بتاريخ: 2023.08.21، الساعة: 00:40.

كذلك من مميزات دفتر التوفير بشريحة مغناطيسية، الراحة التامة في إدارة الأموال عبر الإنترنت، سهولة العمليات المصرفية، توفير الأموال باستمرار.

- **خدمة المونيغرام: Moneygram Service**

هي خدمة تسمح بتحويل أموال العملاء بطريقة سهلة وسريعة من أي بلد بالخارج إلى الجزائر من أجل استلام أموالهم من خلال وكالات بنك التنمية المحلية المتواجدة عبر كامل التراب الوطني.

الشكل رقم (II–13): خدمة المونيغرام



المصدر: www.bdl.dz بتاريخ: 2023.08.21، الساعة: 01:20.

مثلا: بنك التنمية المحلية BDL يقدم هاته الخدمة بالاشتراك مع شركة مونيغرام وهي الشركة الرائدة عالميا في خدمة تحويل الأموال على الصعيد العالمي عبر شبكتها من أجل توفير الطريقة المضمونة، الآمنة والسريعة، لإرسال واستلام الأموال من جميع أنحاء العالم، بشرط الحد الأقصى لعملية إرسال أو استلام الأموال هو 100 ألف دينار جزائري في الجزائر، هاته الشركة لديها أكثر من 350 ألف وكيل منتشر في أكثر من 200 دولة، مقرها بالولايات المتحدة الأمريكية بمدينة دالاس.[1]

المبحث الثالث: ثقة العملاء في الخدمات الإلكترونية المصرفية

التطور والازدهار السريع الذي نشاهده في مجال تكنولوجيا المعلومات والاتصال، انعكس على الخدمات الإلكترونية المصرفية بأشكالها المختلفة، وعلى الرغم من الفوائد المتنوعة التي توفرها هذه الخدمات فهي لم تخلو من المخاطر الحادقة المحيطة بها، ولأجل الاستثمار الجيد في هذا المجال للحصول على نتائج مرضية للطرفين، يجب التركيز على آليات وتدابير تُعزز من ثقة العملاء وتقلص فجوتها.

المطلب الأول: فجوة الثقة في الخدمات الإلكترونية المصرفية

بعد ظهور شبكة المعلومات الدولية بسبب تطور تقنيات الإعلام والاتصال، برزت أنشطة جديدة بما فيها التجارة الإلكترونية، الخدمات الإلكترونية المصرفية ، وعدة أنشطة رقمية مختلفة، بحيث تغيَرت المعاملات المالية تدريجيا من النمط التقليدي إلى النمط الحديث، وهذا ما نتج عنه من وفرات في الوقت والجهد والتكلفة ودقتها في إنجاز الأعمال، بمعنى رفاهية ونمو الاقتصاد بشكل عام، وعلى الرغم من المزايا التي تحققها سواء للعملاء أو للمؤسسات، إلا أن لها مخاطر أدت إلى وجود فجوة ثقة لدى عملائها حالت دون رواجها بالقدر الذي تستحقه.

وتداركا لذلك يجب تدنية هاته الفجوة من خلال إضفاء آليات وتدابير على الأنظمة الإلكترونية (SysTrust)، والمواقع التجارية على شبكة الإنترنت (Web Trust)، واتخاذ مجموعة من المبادئ والمعايير والالتزام بها عند أداء هاته الخدمة بغية تدنية فجوة الثقة في بيئة تتسم بالافتراض.

من خلال نظم المعلومات الإلكترونية يتم تشغيل العديد من التطبيقات، وبالنسبة لمعظم العملاء الذين يتعاملون مع المصرف إلكترونيا، فإن نظم المعلومات تعبر عن قوة وأهمية المصرف لديهم، حيث أن جودة ودقة تلك النظم تميزها في السوق، كما قد تضفي على سمعتها إذا ما كان لتلك النظم مشاكل مختلفة، وبالتالي ينتج ضعف إمكانية الاعتماد عليها، وتخلق فجوة ثقة للعملاء، على سبيل المثال: دراسة أجراها معهد أمن المعلومات (Security Information Institute) سنة 2000 وجد أن 90% من الذين شملتهم الدراسة عانوا

[1] ديدوش هجيرة، حريزي عبد الغني، **نفس المرجع السابق**، ص 29.

من ثغرات في أمن الحاسبات، و74% اعترفوا بوجود خسائر مادية نتيجة لتلك الثغرات، و25% وجدوا أن تلك الثغرات هي نتيجة اختراقات خارجية، هذا وأن مجموع الخسائر كان 250 مليون دولار،[1] وفي إحصائيات أخرى لسنة 2021 تشير إلى تزايد سنوي للخسائر المالية الناجمة عن اختراق البنوك والمؤسسات المالية والمصرفية، حيث أشار تقرير صادر من Advisor Scam إلى أن عدد بلاغات الاحتيال المالي لسنة 2021 وصل إلى 293 مليون بلاغ، مسببة خسائر مالية بلغت 55 مليار دولار أمريكي.[2]

على مستوى العالم هناك زيادة ونمو في العمليات المصرفية الإلكترونية ولكن تبقى منخفضة لا تتناسب مع عدد الأفراد المستخدمين لشبكة الإنترنت، حيث تشير العديد من الدراسات إلى أن نسبة تتراوح بين 35% إلى 40% فقط من المتعاملين لديهم الرغبة في إتمام عمليات الشراء عبر شبكة الإنترنت، ويرجع السبب في ذلك إلى أن غالبيتهم يمارسون التجارة الإلكترونية بشكل جزئي وغير كامل، بمعنى يستخدمون الشبكة للبحث ومقارنة السلع والخدمات ثم يُتمونها بالطرق التقليدية، والسبب الحقيقي لذلك هو انخفاض درجة الثقة في المواقع التجارية ذاتها من حيث الإجراءات المتبعة لإتمام العمليات التجارية ومدى حماية بيانات العملاء واحترام خصوصيتها، وبالفعل ما حدث سنة 2022 يؤكد ذلك، أين تم تسريب 1.2 مليون رقم بطاقة ائتمان مصرفية، وسرقة 9.7 مليون من معلومات وبيانات الأشخاص في تأكيد من بنك: MediBank.[3]

عالم الافتراض وانعدام وجود مكان محدد لإتمام التعاقد في مختلف الأنشطة المالية إلكترونيا عبر شبكة الإنترنت، سبب من أسباب وجود فجوة الثقة عند بعض الأفراد، حيث ينظرون لشبكة الإنترنت بخوف وعدم ثقة كأي تكنولوجيا جديدة، والتخوف من أن تكون بعد المعاملات المالية وهمية، والتخوف من إعطاء أرقام بطاقات الائتمان خوفا من سحب الرصيد، والسرقة والاحتيال، والإحساس بالمخاطر في إتمام الصفقة وما تعلق بجودة السلع أو الخدمات، فوفقا لدراسة تمت سنة 2022، صادرة عن شركة Bromuim الأمريكية المتخصصة في أنظمة الحماية من الفيروسات، بيَنت أن ما بين 45% إلى 50% من جميع التجارة غير المشروعة للمعلومات والبيانات الشخصية هي تشمل بيانات بطاقات الائتمان المصرفية المسروقة بكلمات المرور.[4]

من هنا يتضح أن نقص الثقة بين الأطراف المتعاملة في الأنشطة المالية الرقمية المختلفة، والتخوف، ونقص الأمان والتجربة السابقة، والمعلومات الموثوق فيها عن تلك الأنشطة يمثل فجوة ثقة، فأصبح من الضروري للطرف الأول أن يعطي أهمية كبيرة لبيانات العملاء مع إيجاد آلية يتم إعلامهم بها بحدود استخدام تلك البيانات وكيفية

[1] Pugliese Anthony, Halse Ronald, **SysTrust and WebTrust Technology Assurance Opportunities**, CPA Journal, 2000, Available from: www.nysscpa.org/cpajournal/2000/1100/features/f1128.htm, Retrieved: 01-03-2022, 22:10.

[2] الموقع: https://www.arabiya.net، تاريخ الاطلاع: 20-08-2023، على الساعة: 10:00.

[3] الموقع: ttps://www.websiterating.com، تاريخ الاطلاع: 20-08-2023، على الساعة: 11:00

[4] الموقع: https://www.addustour.com، تاريخ الاطلاع: 20-08-2023، على الساعة: 14:30.

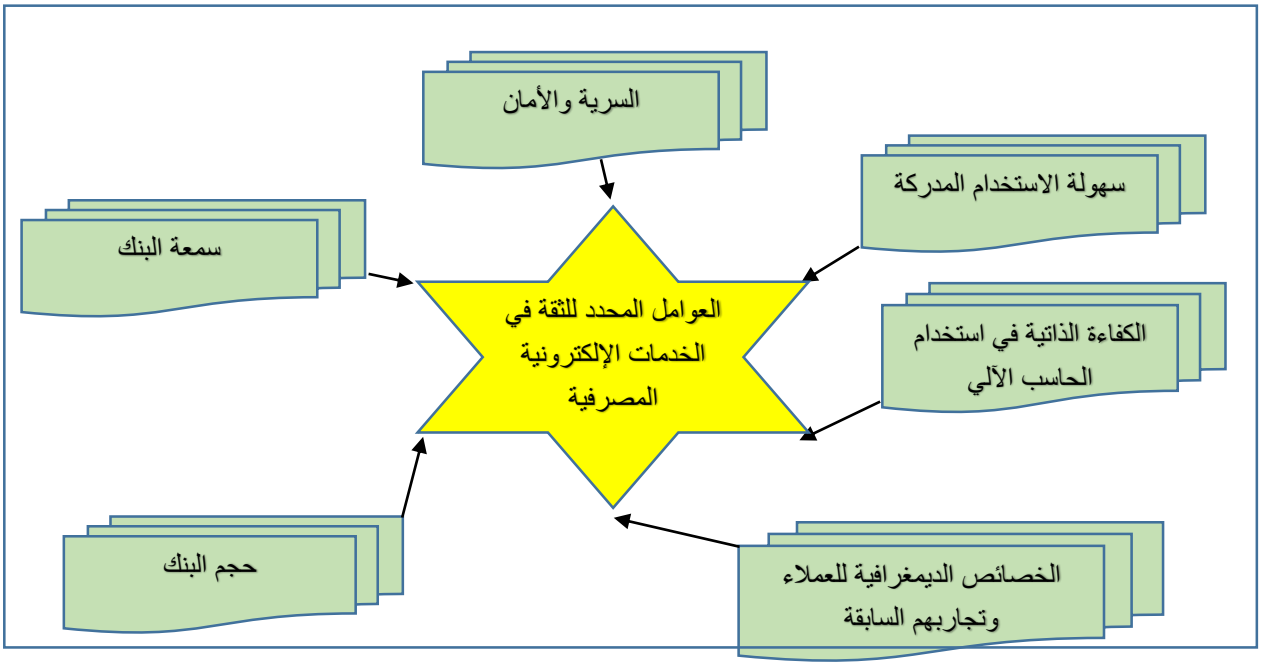
حمايتها والحفاظ عليها، إضافة إلى ضرورة وجود طرف ثالث موثوق فيه يقوم بدور الوسيط بين العملاء والبائعين، حيث يمد العملاء بمعلومات موثوق فيها عن البائعين، ويدعم الثقة بين الطرفين، وهذا ما أدى إلى ظهور جهات أخرى ومؤسسات تقوم بتقديم خدمات إضفاء الثقة الإلكترونية وتضييق فجوتها مثل المؤسسات التالية:

"WebTruste, BBBonline, VeriSing, International Computer Security, NCSA, SusTrust".[1]

المطلب الثاني: العوامل المحددة للثقة في الخدمات الإلكترونية المصرفية

اهتمت البحوث التسويقية كثيرا بعنصر الثقة كمتغير تسويقي مهم في بناء العلاقة بين مختلف المؤسسات والعملاء، حيث ظهرت تيارات فكرية حديثة تركز على المتغيرات المفسرة للثقة في التعاملات الإلكترونية، لما تكتسيه معرفة هذه العوامل من أهمية لدى المسوقين في سبيل كسب ثقة المستهلكين، حيث تُظهر الدراسات أن هناك ستة أنواع لهاته العوامل كما هي موضحة في الشكل أدناه:

الشكل رقم (II–14): العوامل المحددة للثقة في الخدمات الإلكترونية المصرفية



المصدر: من اعداد الطالب بالاعتماد على: صلاح الدين محمد علي، كيفية توفير عنصر الأمن والسرية للمعاملات المصرفية عبر شبكة الإنترنت في المصارف السودانية، دار المنظومة، العدد 73، 2016، ص 38–41، رابط الموقع: https://seaech.mandumah.com/Record/630109، تاريخ الاطلاع: 05–09–2022، على الساعة: 23:20.

[1] محمد المهدي الأمير، عبد الرحمان يوسف الخليفة، صلاح علي أحمد محمد، **أثر التحول لنظام المحاسبة الرقمية على خاصية التمثيل الصادق للمعلومات المحاسبية في ظل مبادئ ومعايير موثوقية الموقع الإلكتروني**، مجلة أرصاد الراسات الاقتصادية والإدارية، السودان، المجلد 04، العدد 02، ديسمبر 2021، ص 18.

من خلال الشكل أعلاه، سنتطرق بشرح وجيز لكل عامل من العوامل المحددة للثقة في الخدمات الإلكترونية المصرفية كما يلي:[1]

1-السرية والأمان: تعد السرية ومدى توفر عنصر الأمان من المواضيع المهمة في أي معاملات مصرفية تتم عبر الإنترنت، وتتحقق السرية والأمان من خلال العديد من التطبيقات التكنولوجية الحديثة والبرامج المتطورة، واستخدام الوسائل الأمنية الخاصة من بينها: التشفير الذي يضمن تبادل المعلومات والبيانات بأمان تام عبر الشبكات، والتصديق الرقمي، والشهادات الرقمية، والبصمة الرقمية، وجدار النار، كلها من أدوات التأمين أثنا إتمام المعاملات المصرفية، بالإضافة إلى وجود موقع آمن للمعاملات المصرفية يحتوي أجهزة خدمة محصنة ضد الاختراقات ومزودة ببرامج وتكنولوجيا تشفير متقدمة تحفظ سرية المعلومات من خلال استخدامها لتكنولوجيا تعرف باسم Secure Socket Layer (SSL) أو طبقة التجويف الآمن، وكذا التوثيق الرقمي الذي يعمل على زيادة درجة الأمن في أي جهاز خدمة محصن بالفعل، فالتوثيق الرقمي يعمل على زيادة مستوى السرية ويضمن أن جهاز الخدمة الذي يتلقى المعلومات هو الجهاز الصحيح، واستخدام الذاكرة الداخلية الانتقالية الحاجزة والشبكة الافتراضية الخاصة لمنع المستخدمين غير المخولين من الدخول إلى الشبكة، وبهاته الطريقة لا يستطيع أحد التحايل على الشبكة بإعادة توجيه عملية النقل إلى موقعه وسرقة البيانات والمعلومات المنقولة.

2-سهولة الاستخدام المدركة: تعرف سهولة الاستخدام بأنها الدرجة التي يعتقد فيها الشخص أن استخدام نظام معين سيكون خاليا من الجهد البدني والعقلي.[2]

3-سمعة البنك: عبارة عن انطباع إجمالي مشترك أو إجماع حول ماذا ستسلك المؤسسة المواقف المحددة، والسمعة تقوم على مجموعة من المعتقدات التي يحملها الفرد حول قدرة المؤسسة ورغبتها في تحقيق مصالح مختلفة الأطراف ذوي الصلة بها، وهناك عدة دراسات ركزت نسبيا وبشكل غير مباشر عل تأثير سمعة المؤسسة في اتجاهات العملاء وسلوكياتهم في الأسواق المالية خاصة في مجال الخدمات المصرفية، حيث تعتبر سمعة البنك أحد المحددات الأساسية لاختيار العملاء للبنك المناسب، وينتظر إلى سمعة البنك باعتبارها متغيرا متعدد الأبعاد، فالطريقة التي يتعامل بها الموظفون مع العميل، وملائمة البنك، وقوة مركزه المالي، تعتبر من أهم المؤشرات التي يستخدمها العميل للدلالة على سمعة البنك قبل التعامل معه،[3] ويتعدى تأثير السمعة من اختيار البنك المناسب إلى الثقة في خدماته.

---

[1] صلاح الدين محمد علي، **كيفية توفير عنصر الأمن والسرية للمعاملات المصرفية عبر شبكة الإنترنت في المصارف السودانية**، دار المنظومة، العدد 73، 2016، ص 38-41.

[2] أحمد زياد أدلي، **العوامل المؤثرة في نية واستخدام التعلم الإلكتروني-دراسة ميدانية في شركات القطاع الصناعي في سوريا**، رسالة أعدت لنيل درجة ماجستير في علوم الإدارة تخصص الموارد البشرية، قسم الموارد البشرية، المعهد العالي لإدارة الأعمال، دمشق، سوريا، 2019، ص 41.

[3] ناجي ذيب معلا، **الأصول العلمية للتسويق المصرفي**، دار المسيرة للنشر والتوزيع والطباعة، عمان، الأردن، الطبعة الأولى، 2015، ص 155.

4-حجم البنك: عادة ما يتسم نشاط البنوك كبيرة الحجم بقدر من التنويع مما يجعلها تتعرض لدرجة مخاطر أقل،[1] وعلى هذا الأساس فإن حجم البنك وانتشار فروعه يعطيه القدرة على تطوير وتنويع الخدمات، والانفاق الاستثماري على التكنولوجيا الحديثة التي أصبحت أساس تطوير الخدمات المصرفية، كما علينا أن ننوه إلى أن احتمالات الإفلاس تنخفض في البنوك ذات الحجم الكبير وذلك لامتلاكها إمكانية أكثر في اللجوء إلى الاقتراض بشروط أيسر وهذا ما أثبتته دراسة Gordon عن وجود علاقة طردية ذات دلال إحصائية بين نسبة الاقتراض وحجم البنك، كما تدخل ضمن حجم البنك الاستثمارات الخاصة به فهي تشكل دليلا ملموسا على إرادة الشريك (العميل، المورد، مؤسسة أخرى...) في الاستثمار في العلاقة وهذا محدد قوي للثقة في البنك.

وبهذا فحجم البنك وانتشار فروعه واستثماراته تعتبر من محددات الثقة حيث يدل امتداد المؤسسة على مساحة كبيرة في السوق على أنها كسبت ثقة العملاء وأنها أهل لهذه الثقة، لذا يميل الأشخاص إلى الثقة بالمؤسسات الكبيرة.

5-الكفاءة الذاتية في استخدام الحاسب الآلي: الكفاءة الذاتية هي الاعتقاد أن المرء لديه القدرة على أداء سلوك معين، وهي بناء مهم في علم النفس الاجتماعي، والكفاءة الذاتية لها تأثير على القرارات المتعلقة بالسلوكيات الواجب القيام بها، فالكفاءة الذاتية في استخدام الحاسب الآلي مثلا لها تأثير على قرار العميل بشأن تبني الخدمات الإلكترونية المصرفية من عدمها، وكذلك ينطبق الأمر على مدى ثقته بها.

6-الخصائص الديمغرافية للعملاء وتجاربهم السابقة: وتتمثل الخصائص الديمغرافية في الجنس والمستوى التعليمي والعمر،[2] بالإضافة للعامل المالي المتمثل في الدخل، بحيث تؤثر هاته الخصائص على سهولة استخدام التقنيات الحديثة المشار إليها سابقا، وكذا مقاومة التغيير.[3]

أما بالنسبة للخبرات والتجارب السابقة للعملاء في العمل المصرفي الإلكتروني هي تولد لهم القدرة الكبيرة والثقة التامة وتجعل تصرفهم مفهوم بالنسبة للمصرف، بحكم نجاح سابقيها من تعاملات وتعودهم عليه.

المطلب الثالث: كيفية تعزيز الثقة وتضييق فجوتها في الخدمات الالكترونية المصرفية

أكبر تحدي يواجه البنوك الإلكترونية، هو كيفية تعزيز ثقة عملائه، ولا يتأتى هذا إلا من خلال ما يلي:

- **التنبؤ الاستباقي:**

[1] حمزة جيلاني تومي، مورد تهتان، **أثر كل من حجم البنك، الربحية والسيولة عل هيكل رأس المال في البنوك الجزائرية**، المجلة الجزائرية للاقتصاد والمالية، العدد 9، أفريل 2018، ص 210.

[2] سمير توفيق صبرة، **التسويق الإلكتروني**، دار الاعصار العلمي للنشر والتوزيع، عمان، الأردن، الطبعة الأولى، 2010، ص 70.

[3] سوسن زهير المهتدي، **تكنولوجيا الحكومة الإلكترونية**، دار أسامة للنشر والتوزيع، عمان، الأردن، الطبعة الأولى، 2011، ص50.

إن أحد العوامل التي تعزز من ثقة العملاء في الخدمات المقدمة إليهم من قبل المصرف الإلكتروني، هي تبني إستراتيجيات وأساليب تساعد على تفهم احتياجات العملاء ورغباتهم والتعرف على المشاكل التي يواجهونها، ولذلك يتوجب على المنظمة المصرفية أن تقدم منتجات أو خدمات تتناسب مع احتياجات العملاء ومتطلباتهم، كما يتعين عليها أيضا التعامل مع التحديات التي تواجه العملاء عن طريق تقديم لهم أفضل الخدمات وإيجاد حلول مبتكرة لكافة المشاكل حتى يشعرون بالأمان وبشكل استباقي.

- **صدق المعاملات:**

يتعين على موظفي المصارف الإلكترونية التعامل مع العملاء بصدق وإخلاص، فهذه الصفات تلعب دورا مهما في كسب رضاهم وثقتهم على المدى البعيد، كما يجب عليهم الحرص على تقديم خدمات متميزة باستمرار والالتزام بأداء واجباتهم تجاه العملاء على أكمل وجه، مع توفير الخدمات دون إبراز هدف الجانب المادي البحت، فالمصرف مطالب بالجانب الإنساني كالنصح والإرشاد والتوجيه وكذا الإجابة على استشارات العملاء، بالإضافة إلى الاعتراف بالخطأ في حال تواجده، مع إضفاء الوضوح والشفافية في التعاملات، حيث أن انعدام المصداقية يثر سلبا على الموظف نفسه وعلى المنظمة المصرفية وسمعتها، وبالتالي على ثقة العملاء.

- **التغذية العكسية:**

إن تعزيز التغذية العكسية لاحتياجات ورغبات العملاء من خلال الاستماع لملاحظاتهم وشكاويهم يعد أفضل وسيلة لكسب ولائهم وتعزيز ثقتهم على المدى الطويل، حيث يجب على موظفي المصرف الإصغاء جيدا لملاحظات العملاء والسعي لتطبيقها عمليا، فالموظف المتميز في الوحدة الاقتصادية الناجحة هو الذي يضع نفسه مكان العميل ويتفهم آراءه ووجهات نظره المختلفة، وهذا ما يعزز ثقتهم نحو الخدمات المصرفية.

- **التواصل المستمر:**

يُمكن اعتبار التواصل السيئ أحد الأسباب التي تدفع العملاء إلى البحث عن مصرف آخر يبدي اهتماما أكبر بعملائه ويلبي احتياجاتهم بفعالية أكبر، لذا يتعين على موظفي المصرف الحرص على خدمة العملاء بطريقة سريعة وفعالة وتوظيف أشخاص يتمتعون بمهارات تواصل جيدة والحرص على تزويدهم بدورات تدريبية حول كيفية تقديم خدمات متميزة للعملاء، على سبيل المثال فتح قسم خاص بخدمة العملاء يهدف إلى التواصل معهم عبر مختلف الوسائل والتقنيات الحديثة (الهاتف، البريد الإلكتروني، مواقع التواصل الاجتماعي،...إلخ).[1]

- **العلاقات التفاعلية:**

يتعين على المصرف تبني أساليب وسياسات جيدة تهدف للاحتفاظ بالعملاء وتعزيز ولائهم وإخلاصهم تجاه المصرف، حيث يجب إظهار اهتمام العملاء من خلال التعاطف معهم، والأنشطة والتواصل الدائم والتفاعل معهم على متواقع التواصل الاجتماعي وفي مناسباتهم الخاصة من أجل بناء علاقات وطيدة معهم لكسب ثقتهم ورفع

[1] الموقع: https://www.arabic.cnn.com/business/six-steps-keep-your-clients، تاريخ الاطلاع: 21-08-2023، على الساعة: 23:40.

مستوى رضاهم عن المصرف وخدماته، فتجاهل العملاء وعدم إظهار الاهتمام بهم سلوك يؤدي إلى قطع العلاقات وفرار إلى مصرف آخر يهتم بشؤون العملاء ويتفاعل معهم.

- **تنفيذ الوعود:**

يُعد الإهمال في تنفيذ الوعود التي يقطعها المصرف للعملاء من أخطر السلوكيات التي يجب تجنبها وذلك نظرا لأثرها السلبي على علاقاته مع العملاء، فإن لم يكن المصرف قادر على حل مشكلة العميل خلال فترة قصيرة فيجب أن تصارحه وتشرح له طبيعة المشكلة والوقت الفعلي الذي تحتاجه لحلها والحرص على التواصل معه باستمرار لاطلاعه على سير العملية، فالوعود الكاذبة تؤثر على سمعة المصرف، وتنفيذ الوعود دليل على الاهتمام بالعملاء واحترامهم وبرهان هدفه الاحتفاظ بهم، على سبيل المثال: وعود خدمات ما بعد البيع، وخصم من السعر في حال تجاوز عتبة معينة من المعاملات المصرفية الإلكترونية.[1]

المطلب الرابع: توقعات الثقة في استخدام الخدمات الإلكترونية المصرفية

قد أوضح هونغ (Hong) أن توقعات الثقة تشير إلى المدى الذي يتوقع فيه العميل أن يكون مقدم الخدمة المحتمل جديرا بالثقة فيما يتعلق بعملية شراء معينة عبر الإنترنت، بمعني أن ثقة العميل في مقدم الخدمة هي مؤشر على اختيار العميل لتلك الخدمة،[2] كما أضاف هُو وآخرون (Hu et al) أن ثقة العملاء في خدمات التكنولوجيا المالية لها تأثير قوي على مواقفهم لتبني تلك التكنولوجيا،[3] كما أكدت دراسة مباما وآخرون (Mbama et al) أن هناك مجموعة من السمات التي تؤثر على تجربة العميل للخدمات المصرفية الإلكترونية هي كما يلي : جودة الخدمة، والجودة والوظيفة، والقيمة المدركة، وتخصيص الخدمة، وسرعة الخدمة، ومشاركة الموظف العملاء، والثقة في العلامة التجارية.[4]

وأيضا أكدت دراسة ستيوارت وآخرون (Stewart et al) أن هناك العديد من العوامل مثل أمان البيانات وثقة العملاء وسهولة واجهة تصميم المستخدم التي تؤثر على اعتماد الخدمات الإلكترونية المصرفية، حيث أنه

---

[1] Al nasrawi Hamed, Al tameeni Ali, **Thabit Thabit**, **Then Impact of Organizational Dogmatism in Reducing the Employees Internal Marketing**, Internasional Journal of Social Sciences Educational Studie, V 05, N 01, 2018, P 18.

[2] Hong Ilyoo, **Understanding the Consumers online marchant selection Process**: **The roles of Product Involvement**, **Perceived Risk**, **and Trust Expectation**, International Journal of Information Management, Vol 35, N 3, 2015, P148, https://doi.org/10.1016/j.ijinfomgt.2015.01.003.

[3] Hu Zhongqing, Ding Shuai, Chen Luting, Yang Shanlin, **Adoption Intention of Fintech Services for Bank Users**: **An Empirical Examination with an Extended Technology Acceptance Model**, Symmetry, Vol 11, N 3, 2015, P 340. https://doi.org/10.3390/sym11030340.

[4] Mbama Cajetan Ikechukwu, Ezepue Patrick Oseloka, Alboul Lyuba, Beer Martin, **Digital Banking**, **Customer Experience and Financial Performance**, **Journal of Research in Interactive Marketing**, Vol 12, N 4, 2018, P 432. https://doi.org/10.1108/JRIM-01-2018-0026.

عندما يزداد ثقة العملاء يعزز ذلك من تبنيهم للتكنولوجيا المالي،[1] كما أضافت دراسة شونج وآخرون (Chuang et al) أن الثقة في العلامة التجارية والثقة في الخدمة لهما تأثير إيجابي معنوي على المواقف تجاه استخدام خدمات التكنولوجيا المالية.[2]

وتُشير نتائج دراسة جونجر وميتزنر (Junger and Mietzner) إلى أنه يؤثر كل من مستوى ثقة الأسرة وراحتها بالتقنيات الجديدة، والمعرفة المالية، على ميلهم إلى التحول إلى التكنولوجيا المالية.[3] كما أكدت دراسة نانجين وآخرون (Nangin et al) إلى أنه من أجل زيادة معدل اعتماد التكنولوجيا المالية، يجب بناء ثقة العملاء، كما أثرت الثقة بشكل إيجابي على نية تبني التكنولوجيا المالية الإسلامية في باكستان، حيث أنه كلما زادت ثقة العملاء في التكنولوجيا المالية الإسلامية، زادت النية في تبنيها، وقد يكون التضمين المحتمل لهذه النتيجة هو أن العميل يعتبر الثقة عاملا مهما قبل استخدام التكنولوجيا المالية،[4] أما كونلولي (Connolly) أشار إلى أن ثقة العميل أصبحت أكثر أهمية من أي وقت مضى، حيث لم تعد الوسائل التقليدية لبناء الثقة والحفاظ عليها فعالة بسبب العدد الهائل لمنصات الخدمات الإلكترونية المصرفية والوضع التنافسي لها، لذلك أصبح لزاما على الشركات البحث عن طرقا جديدة لبناء ثقة العميل في الخدمات الإلكترونية،[5] بالإضافة إلى ذلك، أضافت دراسة علي وآخرين (Ali et al) إلى أنه يشير مستوى ثقة العملاء إلى أن لديهم تصورا أكثر إيجابية عن التكنولوجيا،[6] كما أضافت دراسة سرجيوس إلى أن سهولة استخدام الموقع والتصفح والبحث وانخفاض وقت التحميل يؤول إلى الثقة ومن تكوين اتجاه إيجابي نحو نية العملاء للشراء الإلكتروني.[7]

---

[1] Stewart Harrison, Jurjens Jan, **Data Security and Consumer Trust in FinTech Innovation in Germany**, **Information and Computer Security**, Vol 23, N 1, 2018, P 109. https://doi.org/10.1108/ICS-06-2018-0039.

[2] Chuang Limin, Kao Hsiao, Liu Chun, **The Adoption of Fintech Service**: **TAM Perspective**. International Journal of Management and Administrative Sciences, Vol 3, N 7, 2016, P 15.

[3] Junger Moritz, Mietzner Mark, **Banking Goes Digital**: **The Adoption of FinTech Services by German Households**, Finance Research Letters, 2020, P 34. https://doi.org/10.1016/j.frl.2020.08.008.

[4] Nangin Meryl Astin, Barus Irma Razita Gloria, Wahyoedi Soegeng, **The Effects of Perceived Ease of Use**, **Security**, **and Promotion on Trust and Its Implications on Fintech Adoption**, Journal of Consumer Sciences, Vol 5, N 2, 2020, P 138. https://doi.org/10.29244/jcs.5.2.124-138.

[5] Connolly Barry, **Same as Previous Reference**, P 63.

[6] Ali Muhammad, Syed Ali Raza, Puah Chin Hong, Amin Hanudin, **How Perceived Risk**, **Benefit and Trust Determine User Fintech Adoption**: **a new Dimension for Islamic Finance**, Foresight, Vol 23, N 4, 2021, P 403. https://doi.org/10.1108/FS-09-2020-0095.

[7] اسكندر سرجيوس، أنطوان، **تأثير جودة الموقع الإلكتروني على النية نحو الشراء: في ظل الدور الوسيط للثقة في الموقع والاتجاه نحوه**، مجلة جامعة الإسكندرية للعلوم الإدارية، العدد 68، رقم 6، 2021، ص 155. الموقع: https://dx.doi.org/10.21608/acj.2021.204475

المطلب الخامس: نتائج ثقة العملاء في استخدام الخدمات الإلكترونية المصرفية

ينتُج عن ثقة العملاء في استخدام الخدمات الإلكترونية المصرفية مجموعة من النتائج هي:

- ✓ **الرضا:** وهو عبارة عن إحساس العميل الناتج عن حُكم مُقارن بين أداء المنتج وبين توقعاته،[1] بمعنى هو شعور العملاء بالسرور والارتياح حين يقارن أداء الخدمة المصرفية الإلكترونية التي يحصل عليها فعلا بالتوقعات التي يحملها عن هذه الخدمات من قبل، فمن حيث الناحية الشعورية نلتمسها في عملية الاستجابة الإيجابية للمؤسسة، ومن الناحية الإدراكية تكون بالشعور الإيجابي للعملاء الناتج عن تقييم جوانب العلاقة مع المؤسسة وممثليها كمقدمي الخدمات وسلوكهم التعاوني ومقارنتها بالتوقعات، أي مدى تعويض المنتج أو الخدمة بطريقة ملائمة للتضحيات المقدمة لنيله، حيث إذا جمعنا بين الناحية الإدراكية والشعورية يكون الرضا ظاهرة غير ملاحظة أي حالة نفسية ناتجة عن التجربة والمقارنة مع التفضيلات الأساسية، فالرضا يُعتبر أحيانا على أنه انفعال وتأثر بخصائص المنتج أو الخدمة، فهو يُشجع على بناء علاقة الثقة، كما أن الثقة بدورها تُؤدي إلى زيادة مستوى الرضا بالخدمات وجودتها وبهذا يقوده إلى تشكيلة نية إعادة الشراء، وفي الجهة المقابلة من الممكن أن يُؤدي الرضا في حالة ما إذا كان سالبًا إلى عدم الرضا الذي ينتُج عنه نفور العملاء والكف نهائيًا عن شراء المنتج أو الخدمة، أما إذا كان مستوى الرضا متوسط فمن الممكن أن يتحول العملاء إلى مؤسسات أخرى، وبهذا فالرضا هو ينتُج عن الثقة.
- ✓ **الولاء:** وهو التزام عميق للعملاء بإعادة شراء الخدمة في المستقبل رغما عن المؤثرات الخارجية المحيطة، والجهود التسويقية التي تسعى إلى محاولة تغيير قرار الشراء، ويظهر سلوك الولاء جليا من خلال دراسة العلاقة بين العملاء والمنظمة ففي البداية يكون العميل محتملا (يمكن أن يقوم بعملية الشراء ويمكن لا يقوم)، فالمصرف يُحاول تشجيع هذا العميل للقيام بأول عملية شراء حتى يُصبح عميل جديد، ويتواصل تشجيعه له كي يُعيد الشراء عدة مرات وهنا يصبح بينه وبين المصرف علاقة كبيرة تتصف بالثقة، ونتيجة ذلك يصبح العميل لا يشتري فحسب بل يقوم بالإشهار لخدمات البنك ونشر خبرته الإيجابية بالكلمة المنطوقة الإيجابية الحسنة، فكسب ولاء العملاء والحفاظ عليهم هدفه ونتيجته تخفيض تكلفة الحصول على عملاء جدد، وأيضا تحقيق الأرباح على المدى الطويل، لذلك يعتبر الولاء هو ناتج عن ثقة العملاء.
- ✓ **الالتزام المتبادل:** أي أن المؤسسة المصرفية تقدم خدمة معينة بدقة لعملائها وبشكل يمكنهم من الاعتماد على هذه المؤسسة، حيث تتأثر ثقة العملاء بدرجة الالتزام المتبادل، وتعرف كإرادة من الطرفين للمحافظة على علاقة ثقة قوية ودائمة ومتابعتها على المدى الطويل، وزيادة التفاعل بين الطرفين، وزيادة ربحية الخدمات

[1] منير نوري، **سلوك المستهلك المعاصر**، ديوان المطبوعات الجامعية للنشر والتوزيع، الجزائر، 2013، ص 314.

الإلكترونية المصرفية التي يقدمها المصرف، فالثقة تؤدي إلى الرغبة في مواصلة العلاقة وتُعزز قيمتها وتساهم بصفة كبيرة في الرغبة بالالتزام، وتوجد ثلاثة صيغ للالتزام وهي:[1]

- ❖ **الالتزام العاطفي (Affective Commitment)**: هذا الالتزام يشير إلى رغبة وطموح العميل في الاستمرار في العلاقة وإطالتها قدر الإمكان والتعامل مع الطرف الآخر، وهذا ناتج من التعلق العاطفي بهذه العلاقة والذي ينشأ من فهم ومشاركة وتحديد طرف لقيم الطرف الآخر.
- ❖ **الالتزام الحسابي (Calculative Commitment)**: ويشير إلى رغبة العميل في الاستمرار بالتعامل مع المنظمة، وأن هذه الرغبة تعود إلى تقييمه المعرفي للقيمة التي سيحصل عليها من هذه العلاقة من فوائد وإيجابيات عند الاستمرار في هذه العلاقة، وكذلك الخسائر والسلبيات التي سيواجهها عند إنهاء هذه العلاقة.
- ❖ **الالتزام المعياري (Normative Commitment)**: ويشير إلى شعور العميل بأنه يجب الاستمرار في هذه العلاقة نتيجة لبعض المعايير التي يضعها والتي تتشابه مع القواعد والمعايير التي تلتزم بها المنظمة التي يتعامل معها.

- ✓ **التبادلية**: تُبين الكثير من الدراسات والنظريات الاجتماعية أن التبادل هو أساس العلاقة ويُفترض فيه العطاء والأخذ ثم العطاء، مثلا: عندما يتبادل المصرف الإلكتروني والعميل خدمة معينة ينتُج عن ذلك إلزامية شعورية بتكرار التبادل، فحين يشتري المصرف الورق لمتطلبات العمل من مؤسسة تنتج الورق، في حين هذه المؤسسة يُقدم لها المصرف خدمة قرض عمل، فمن خلال ثقة العملاء في المصرف فإنهم يستفيدون من الخدمات المصرفية، ويستفيد المصرف هو الآخر من تحسُن صورته الذهنية.
- ✓ **التفاعل**: يتطلب التفاعل وجود بُعدين أساسيين هما: التعامل المادي كإتمام عملية الشراء أو الخدمة أو الصفقة التجارية، والاتصال الشخصي مع العميل بما يؤدي إلى ترك أثر طيب لديه سواء كان هذا العميل فردا أو ممثلا لمؤسسة، ومن هنا يبقى العميل في تفاعل مع المؤسسة وتعامل معها بديمومة واستمرار، وبهذا يكون التفاعل ناتجا هو الآخر عن الثقة.[2]

[1] Lombard Roberts, Tonder Estelle, Pelser Theuns, Prinsloo Johannes, **The Relationship Between Key Variables and Customer Loyalty Within the Independent Financial Advisor Environment**, The Retail and Marketing Review, Vol 10, N 01, 2014, P 29.

[2] زهرة خلوط، **التسويق الابتكاري وأثره على بناء ولاء الزبائن**، رسالة ماجستير، تخصص تسويق، الجزائر، 2014، ص 25.

خلاصة الفصل الثاني:

تُعتبر الثقة أمرا أساسيا في عصر التكنولوجيا الرقمية، خاصة إذا ما تعلق الأمر بالقطاع المالي وما يقدمه من خدمات مختلفة على وجه العموم وخدمات مصرفية إلكترونية على وجه الخصوص، فالتطور النسبي لهاته الأخيرة باستخدام بطاقات الدفع والسحب الإلكترونية ونمو حجم المعاملات المالية المختلفة عبر شبكة الإنترنت في الجزائر، لزال لم يرقى للمستوى المطلوب، هذا ما دفعنا للبحث عن أسباب الاقبال البطيء للعميل الجزائري نحو مثل هاته المعاملات وما يعزز ثقته نحوها، عليه خصصنا هذا الفصل للحديث عن الأدبيات النظرية التي تشكل الإطار المفاهيمي لثقة العملاء في الخدمات الإلكترونية المصرفية، حيث في المبحث الأول قمنا بتعريف الثقة والتطرق إلى اختلاف الثقة العادية عن الثقة الرقمية، ثم تحدثنا عن خصائص الثقة وأهميتها في الخدمات الإلكترونية المصرفية، وذكر أبعادها ومؤشراتها وأدوات قياسها، ثم تفصيل مراحل بناء ثقة العملاء وطرق تعزيزها، لننتقل للحديث في المبحث الثاني عن الخدمات الإلكترونية المصرفية ، من خلال التعاريف المختلفة المقدمة لها، وتبيان أهميتها ومزاياها ومتطلبات نجاحها، ثم التطرق إلى نظام الدفع الإلكتروني وأنوع الخدمات الإلكترونية المصرفية، أما في المبحث الثالث المتعلق بثقة العملاء في الخدمات الإلكترونية المصرفية، قمنا بتعريف فجوة الثقة في الخدمات الإلكترونية المصرفية، ثم شرح العوامل المحدد لهاته الثقة وكيفية تعزيزها وتضييق فجوتها، ثم الحديث عن توقعات الثقة في استخدام الخدمات الإلكترونية المصرفية، وتحليل أهم النتائج المتحصل عليها من خلال هاته الثقة، وقلنا أن هاته الأخيرة من أجل الوصول إليها، المصرف مطالب بحسن بنائها من خلال إستراتيجية واضحة عنوانها توعية العملاء مع المزيد من إجراءات تعزيزها وتقويتها.

القسم الثاني

الدراسة الميدانية لدى عينة عملاء بنك التنمية المحلية غرداية

الفصل الأول

منهجية الدراسة الميدانية

تمهيد:

بعدما تناولنا في الفصلين السابقين أهم المفاهيم والأدبيات النظرية، سنحاول في هذا الفصل إسقاط الجانب النظري على أرض الواقع، وذلك من خلال دراسة ومحاولة بناء نموذج لتفسير تأثير الأمن السيبراني في الخدمات الإلكترونية المصرفية من خلال تعزيز ثقة العملاء لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية، وهو ما سنحاول دراسته ميدانيا.

متناولين في الدراسة الميدانية ثلاثة مباحث كما يلي:

- المبحث الأول: منهجية البحث والبنك محل الدراسة الميدانية.
- المبحث الثاني: تصميم أداة الدراسة وأساليب جمع ومعالجة البيانات.
- المبحث الثالث: اختبار أداة الدراسة والنموذج النظري العام المقترح للدراسة.

المبحث الأول: منهجية البحث والبنك محل الدراسة الميدانية

تندرج هذه الدراسة ضمن الدراسات الميدانية الوصفية الاستكشافية، لذلك سنعتمد المنهج البحثي المناسب في مثل هذه الدراسات بهدف الوصول إلى نتائج دقيقة وموثوقة.

المطلب الأول: منهج، مجتمع وعينة الدراسة

أولا: المنهج المعتمد في الدراسة

انتهجت الدراسة المنهج الوصفي التحليلي الذي يصف الظاهرة المدروسة وصفاً كمياً وكيفياً من خلال جمع المعلومات وتصنيفها، ومن ثم تحليلها وكشف العلاقة بين أبعادها المختلفة من أجل تفسيرها تفسيرا كافياً والوصول إلى استنتاجات عامة تسهم في فهم الحاضر وتشخيص الواقع وأسبابه.

- **الأسلوب الوصفي** في بعض أجزاء البحث بتكوين القاعدة النظرية المستقاة من مختلف المراجع، ويعتبر الأسلوب الوصفي مناسبا لتقرير الحقائق والتعريف بمختلف المفاهيم ذات الصلة بالموضوع.
- **الأسلوب التحليلي** لنتائج الدراسة الميدانية ومعرفة مدى مساهمة أبعاد الأمن السيبراني للبيانات في تعزيز ثقة العملاء نحو الخدمات الإلكترونية المصرفية، واستخلاص النتائج التي تخدم أغراض هذا البحث، حيث اعتمدت الدراسة على نوعين من البيانات هي:

- **البيانات الثانوية:** وهي مراجعة الأدبيات الواردة في المصادر والمراجع ذات الصلة بالموضوع والدراسات السابقة والتي ساعدت الباحث في التوجيه المفاهيمي وتحديد متغيرات الدراسة.
- **البيانات الأولية:** فهي التي اعتمدت الدراسة عليها بشكل مباشر في الإجابة على الإشكالات المطروحة واختبار فرضيات الدراسة، وقد تم توفير تلك البيانات اعتمادا على أداة الدراسة المتمثلة في الاستبانة.

ثانيا: مجتمع الدراسة:

يعرف مجتمع الدراسة على أنه المجموعة الإجمالية من العناصر التي لديها خصائص مشتركة مع الهدف الأساسي للدراسة ومنه يعمم الباحث النتائج عليه في النهاية، وعليه وبناء على ما سبق فإن مجتمع الدراسة المستهدف حسب دراستنا الحالية، يتكون من مجموعة العملاء المستخدمين لبطاقات الدفع الإلكترونية ببنك التنمية المحلية BDL بولاية غرداية البالغ عدده حوالي: (4700) إلى غاية شهر مارس من سنة 2024، حسب ما أكد لنا عنه المنسق الجهوي للدفع الإلكتروني السيد/ "**محمد فسيو**" المكلف بالوكالة، من خلال اعتمادهم في الإحصاء على البطاقات المحينة فقط.

ثالثا: عينة الدراسة:

كقاعدة عامة يجب أن يكون الحد الأدنى لحجم العينة في نمذجة المعادلات الهيكلية (SEM-PLS) متبعا لقاعدة العشرة أضعاف، وهي كما يلي:

-أكبر بعشرة أضعاف من أكبر عدد من المؤشرات التكوينية المستخدمة لقياس مبني واحد من مباني النموذج.
-أكبر بعشرة أضعاف من أكبر عدد من المسارات الهيكلية الموجهة إلى مبني معين في النموذج الهيكلي.

في دراستنا الحالية فإن أكبر عدد المؤشرات هي التي تقيس المتغير المستقل وعددها خمسة مؤشرات، وعليه فإن الحد الأدنى للعينة المطلوبة وفق نمذجة (SEM-PLS) هي 50 فرد، وعينة دراستنا الحالية تعدت هذا الرقم.

-بالإضافة إلى ذلك فاختيار حجم العينة يعتمد على نوع مجتمع الدراسة إذا كان متجانسا أم لا، وبما أن مجتمع دراستنا متجانس تقريبا، فإننا نكتفي بحجم العينة التي اقتصرت على 195 مفردة من عملاء يتعاملون بواسطة بطاقة الدفع الإلكترونية مع بنك التنمية المحلية، تم اختيارهم بطريقة **عشوائية بسيطة** (كون مجتمع الدراسة متجانس تقريبا، وجميع عناصر المجتمع لها نفس الفرصة في الظهور في العينة، وهذا ما يحقق درجة عالية من الدقة)، حيث تم توزيع 200 استبانة وأسترجع منها 195 استبانة قابلة للمعالجة أي بنسبة استرداد: 97،5%، في حين لم يسترد 02 استبانات نظرا لعدم إرجاعها لنا من قبل الأفراد الذين استلموها منا على أن يتم ملؤها بعد فترة زمنية بحجة الانشغال والقلق لكن دون جدوى، كما أستبعد 03 استبانات كون الإجابات لم تكن كاملة.

جدول رقم (III-1): نتائج توزيع واسترجاع الاستبانة.

الاستبيانات الموزعة		الاستبيانات غير المسترجعة		الاستبيانات المستبعدة		الاستبيانات المقبولة	
التكرار	النسبة المئوية	التكرار	النسبة المئوية	التكرار	النسبة المئوية	التكرار	النسبة المئوية
195	%100	02	%1،02	03	%1،53	195	%97،5

المصدر: من اعداد الطالب بناء على نتائج التوزيع الميداني للاستبانة.

قام الطالب بتوزيع الاستبيانات طيلة أيام الدراسة الميدانية على عملاء بنك التنمية المحلية بولاية غرداية، وهذا بتواجده المستمر بالبنك مستهدفا الشريحة المذكورة أنفا، مع المساعدة القيمة من قبل المنسق الجهوي لبطاقات الدفع الإلكترونية السيد/ محمد فسيو.

المطلب الثاني: تعريف بنك التنمية المحلية بغرداية، أهدافه ومهامه وأنواع البطاقات الإلكترونية الموجودة به

أولا: تعريف بنك التنمية المحلية BDL (Banque de Développement Local):[1]

طبقا للمرسوم رقم: 85-85، المؤرخ في: 1985/04/30 تأسس بنك التنمية المحلية، منبثقا من بنك القرض الشعبي الجزائري CPA، برأس مال قدره: نصف مليار دينار جزائري، يقوم بجميع العمليات مثل: (بنوك الودائع، ضمانات، تقديم القروض، حسابات جارية، خدمات متفرقة)، لكنه يخدم بالدرجة الأولى فعاليات الهيئات العامة المحلية "قروض صغيرة ومتوسطة الآجال، تمويل عمليات الاستيراد والتصدير"، إضافة إلى خدماته للقطاع الخاص (قروض قصيرة ومتوسطة الأجل فقط)، مقره الرئيسي بسطوالي ولاية تيبازة، يعتبر من أوسع الشبكات البنكية على الصعيد الوطني وأحدثها، إذ يعتبر آخر بنك أسس بالجزائر قبل الدخول في مرحلة الإصلاحات، كما يمتلك حاليا شبكة من 155 وكالة عبر الوطن، مقر وكالته بوسط ولاية غرداية بنهج الأمير عبد القادر، باشر عمله سنة 1989، وهو يقوم بجميع العمليات المصرفية على غرار البنوك التجارية الأخرى، يشتغل به 40 موظفا، يتوزعون على مختلف المصالح التالية: (مصلحة الصندوق، مصلحة القروض، مصلحة التجارة الخارجية، مصلحة الرقابة، مصلحة المقاصة).

كما لا يفوتنا أن نشير أن بنك التنمية المحلية غرداية هو وكالة جهوية (مديرية جهوية) تضم (10) عشرة وكالات تابعة لها وهي كل من: (وكالة القرارة، وكالة بريان، وكالة المنيعة، وكالة الأغواط، وكالة تيميمون، وكالة تمنراست، وكالة إليزي، وكالة ورقلة، وكالة تقرت، وكالة حاسي مسعود)، بالإضافة إلى أنه يحتوي على أربعة دوائر في تقسيمه الإداري وهي: (دائرة الإدارة، دائرة المنازعات وتحصيل الديون، دائرة القروض، دائرة الإدارة التجارية)، وبالنسبة لدائرة الإدارة فهي تحتوي على خلية جهوية تقنية للإعلام الآلي.

ثانيا: مهامه وأهداف بنك التنمية المحلية BDL:

جدول رقم (III-2): مهام وأهداف بنك التنمية المحلية BDL

مهام البنك	أهداف البنك
• القيام بالعمليات الاستثمارية المنتجة التي تبادر بها الجماعات المحلية. • قبول الودائع التي قد تكون بعضها تحت الطلب لأجل محدد.	• تحقيق الربح مع توسيع دائرة النشاط. • اكتساب وجلب أكبر عدد ممكن من العملاء من أجل الحصول على عمولات أكبر من الأعمال المرتبطة بالخدمات البنكية المقدمة.

[1] مقابلة مع السيد/ محمد فسيو، المنسق الجهوي لبطاقات الدفع الإلكترونية، بنك التنمية المحلية غرداية، بتاريخ: 02-06-2022، على الساعة: 10:00.

• خدمة فعاليات الهيئات العامة المحلية بالقروض الصغيرة والمتوسطة الآجال. • المساهمة في تمويل المشروعات وذلك من خلال منح القروض. • شراء وبيع الأوراق النقدية وحفظها لحساب المتعاملين معه. • تحويل العملة الأجنبية إلى العملة الوطنية لسداد التزامات العملاء فيما يتعلق بعمليات الاستيراد. • سير عمليات التجارة الخارجية ونشاطات الاستثمار • إنجاز المخططات والبرامج التنموية الوطنية. • تمويل المؤسسات والمقاولات العمومية ذات الطابع الاقتصادي الموضوعة تحت تصرف الهيئات المحلية.	• تحسين التسيير وجعله أكثر فاعلية للتكييف مع التطورات وذلك بإدخال تقنيات حديثة وجديدة في ميدان التسيير والتسويق. • تحقيق توازن اقتصادي ونقدي، قصد تفادي ارتفاع معدلات التضخم. • تقديم الخدمات الشاملة والاستعمال العقلاني للموارد والاستخدامات. • إنشاء سمعة جيدة للبنك وكسب ثقة العملاء. • البحث عن خدمات جديدة للبنك تتماشى مع احتياجات العملاء مثل قروض الاستهلاك. • تنفيذ المخطط والبرامج المقررة لإنجاز الأهداف المرسومة للهياكل والأعمال المحددة مسبقا.

المصدر: من اعداد الطالب اعتمادا على مقابلة المنسق الجهوي لبطاقات الدفع الإلكترونية.

ثالثا: الهيكل التنظيمي لبنك التنمية المحلية BDL:

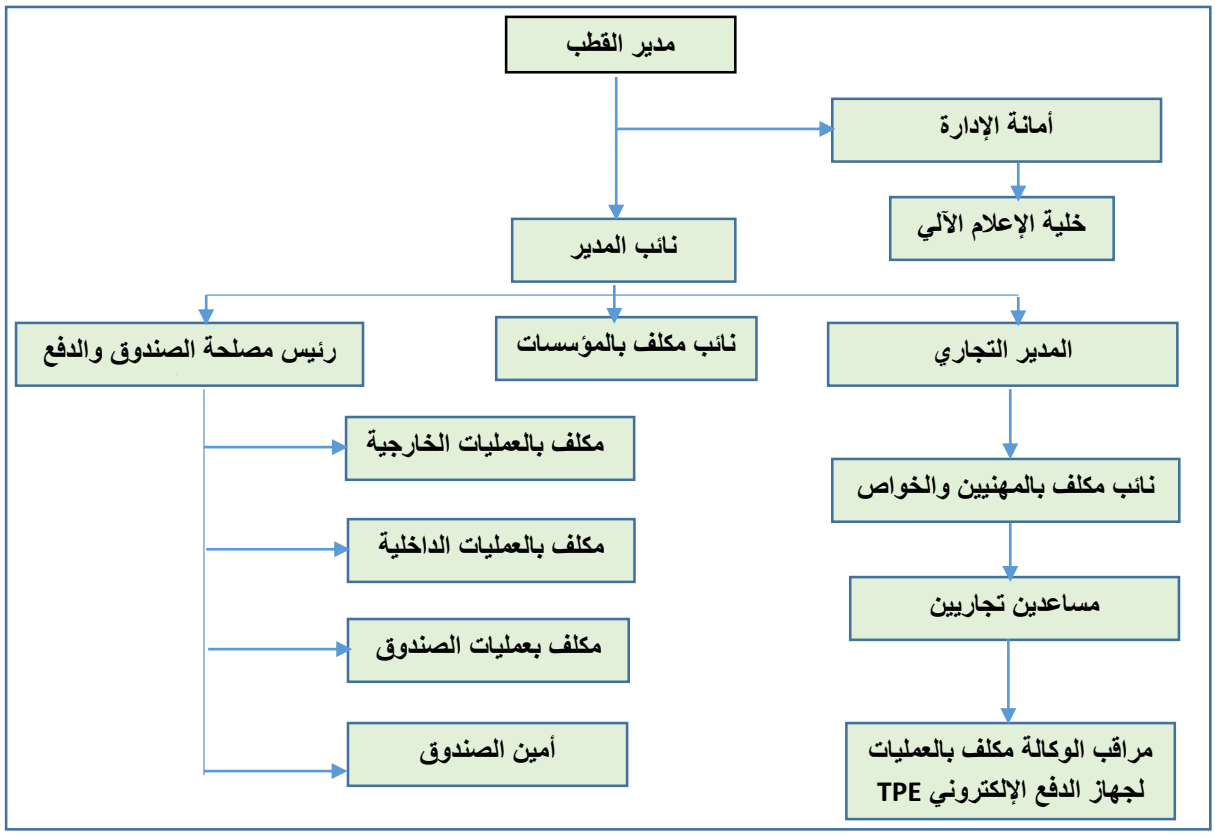
ملتزما بتحقيق المخطط الاستراتيجي 2015-2020 قام بنك التنمية المحلية بوضع هيكل تنظيمي جديد حيث دخل حيز التنفيذ منذ تاريخ: 2017/03/01، من خلاله قام بإعطاء اهتمام أكثر لمفهوم الموارد البشرية، كما ركز على الفصل بين مفهوم الوظائف التجارية والوظائف العملياتية، فقد اختلف عن سابقه بوجود أربع نواب للمدير العام بدل اثنان وتميز أيضا باللامركزية خاصة فيما يخص إعطاء مساحات أكبر للأقطاب التجارية والوكالات التابعة لها في أخذ القرارات المتعلقة بالقروض، حيث قسم إلى ثلاثة مستويات هي:

- المستوى الأول: يتكون من رئاسة المديرية العامة وأربع نواب للمدير العام وكذلك المديريات المركزية.
- المستوى الثاني: بعد أن كان يتكون من مديريات جهوية للاستغلال أصبح يتكون من أقطاب عملياتية وعددها 16 وأقطاب تجارية عددها 35.
- المستوى الثالث: يتكون من الوكالات التجارية التي تقع تحت إشراف الأقطاب التجارية وعددها 155 منها 6 وكالات خاصة بالقرض على الرهن PSG.

وما يهمنا في بحثنا هذا هو مديرية تطوير الشبكة ومديرية الوسائل المادية ومديرية هياكل أمن نظم المعلومات ومديرية الإدارة والصيانة ومديرية التسوية ومديرية الأمن والمحفوظات التي لها علاقة مباشرة بالوكالات التجارية وبسير بطاقات الدفع الإلكترونية وبسلامتها وأمنها.

للإشارة: اعتمدنا في بحثنا هذا على الهيكل التنظيمي للوكالة الجهوية غرداية التي يوجد بها دائرة الإدارة التي تحتوي على خلية تقنية وهي خلية الإعلام الآلي والتي من مهامها صيانة وسير أجهزة الحاسوب ومعالجة بعض المشاكل التقنية، ومتابعة البرامج والتطبيقات، ومدى فعالية الشبكات والبرتوكولات المختلفة.

الشكل رقم (III-1): الهيكل التنظيمي لبنك التنمية المحلية غرداية.



المصدر: من اعداد الطالب اعتمادا على مقابلة المنسق الجهوي لبطاقات الدفع الإلكترونية.

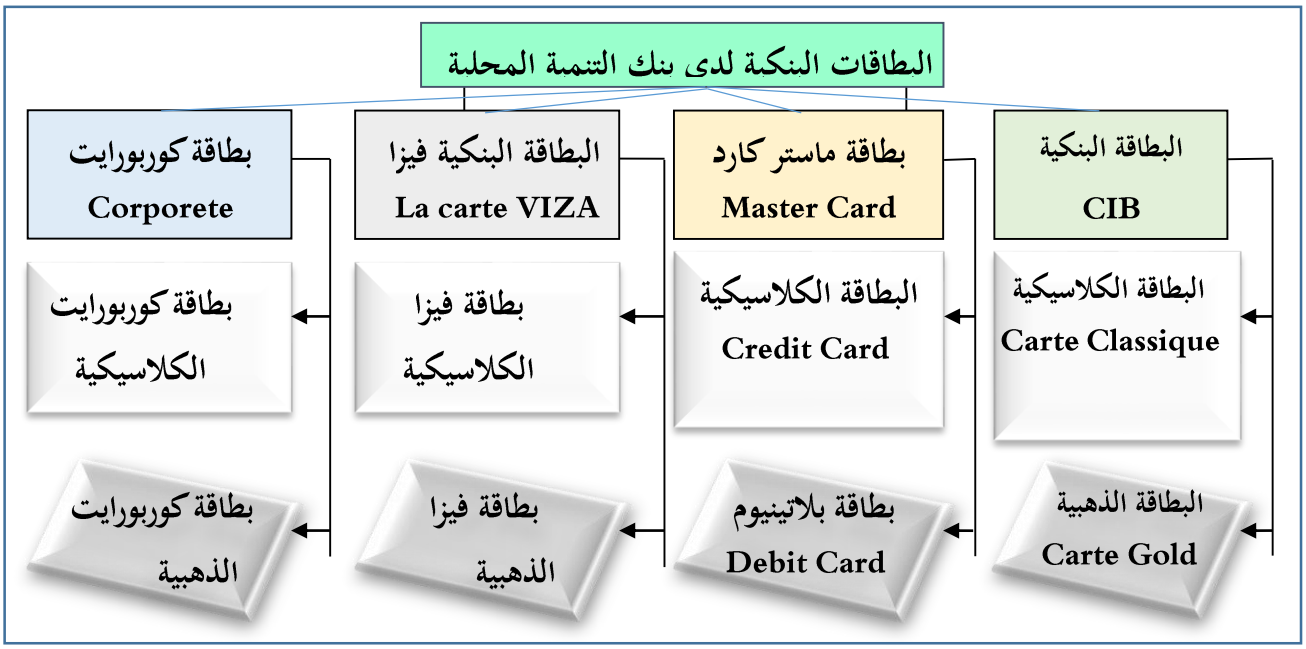
رابعا: أنواع بطاقات الدفع الإلكترونية الموجودة ببنك BDL بغرداية وأهم الخدمات الإلكترونية المصرفية المقدمة من خلالها بطاقات الدفع الإلكترونية الموجودة ببنك التنمية المحلية BDL:

عملت الجزائر كغيرها من الدول على مسايرة التقدم الاقتصادي والتكنولوجي، وذلك بتبني وسائل الدفع الإلكتروني المختلفة التي اتخذت أشكالا تتلاءم ومتطلبات التجارة الإلكترونية وطبيعة المعاملات عبر الإنترنت، فكان أول ظهور لها بخصائص شريط مغناطيسي إلى أن طُورت إلى بطاقة ذات خلية أو شريحة إلكترونية.

بطاقات الدفع الإلكترونية: يطلق عليها أيضا بطاقة الائتمان، بطاقة الوفاء الحديثة، بطاقة الضمان، الحافظة الإلكترونية، وهي بطاقة بلاستكية مصنوعة من مادة كلوريد الفنيل غير المرن، ذات خصائص معينة صادرة عن مؤسسة مصرفية، تستخدمها كوسيلة تعامل عوضا عن النقود (وسيلة وفاء)، ويستطيع حاملها الحصول على النقود

أو التمتع بواسطتها بخدمات مالية إضافية إلى إمكانية استفادته من الائتمان الممنوح بموجبها من المصرف المصدر لها، وذلك لتلبية حاجاته المختلفة أي قد تعتبر في بعض الحالات بمثابة فتح اعتماد بمبلغ لمصلحة صاحب البطاقة حيث يستطيع الوفاء بقيمة مشترياته من السلع التي عليها من طرف التجار المتعاقدين مع البنك"، فهي تمكن حاملها من الحصول على النقود عن طريق آلات الصرف الذاتي (ATM)، على أن يلتزم حاملها بتعبئتها بالمبالغ المحددة في الآجال المتفق عليها، فكان أول ظهور لها سنة 1994 ببنك الفلاحة والتنمية الريفية على شكل بطاقات سحب مقتصرة على بعض الوكالات الخاصة فقط، إلى غاية القفزة النوعية التي شهدتها مجموعة من البنوك الجزائرية سنة 2008، حيث أصبحت تستعمل البطاقات الإلكترونية، وما سنتطرق إليه هو البطاقات الإلكترونية الموجودة ببنك التنمية المحلية غرداية محل الدراسة، حيث قمنا بجمعها في الشكل الموالي كما يلي:

الشكل رقم (III-2): أنواع بطاقات الدفع والسحب الإلكتروني لدى بنك BDL



المصدر: من اعداد الطالب بالاعتماد على الموقع الإلكتروني لبنك التنمية المحلية.

من خلال الشكل رقم (24) سنتطرق إلى كل نوع من أنواع البطاقات الإلكترونية المصرفية الموجودة ببنك التنمية المحلية محل الدراسة الميدانية كما يلي:

1-البطاقة البنكية Carte Inter Bancaire (CIB):

من أحسن البطاقات التي يمكن استعمالها للحصول على أفضل طريقة للدفع وسحب الإلكترونية، وهي بطاقة مشتركة ما بين البنوك داخل التراب الوطني، موصولة بالحساب الشخصي، تتضمن شريحة إلكترونية تضمن أمن عملية الدفع وعملية التسديد لدى مختلف التجار أو الفنادق والمحلات التجارية...الخ، أنشأت هذه البطاقة بالتعاون مع شركة SATIM المنشأة لمشروع نظام الدفع والصانعة للبطاقات (شركة النقد الآلي للصفقات ما

بين البنوك)، تسمح القيام بعمليات السحب والدفع والاطلاع على الحساب بكل سهولة وأمان، ومدة صلاحيتها عامين قابلة للتجديد أوتوماتيكيا، ونجد في هذه البطاقة نوعين هما:

أ- البطاقة الكلاسيكية La Carte Classique: هي بطاقة توفر خدمات الدفع والسحب البنكي وهي تقدم الزبائن وفق شروط يحددها البنك كمداخيل الزبائن أو أهميتهم أو مواصفات أخرى، وللحصول على هذه البطاقة يتم إبرام عقد بين البنك والعميل، كما حدد سقف السحب أو الدفع بواسطتها بـ: 50.000دج في الأسبوع.

ب- البطاقة الذهبية La Carte Gold: هاته البطاقة يتم اختيارها وفق شروط محددة، بالإضافة إلى خدمات الدفع والسحب هي توفر خدمات إضافية مع سقف سحب ودفع مرتفع نسبيا، وتمنح للأشخاص المهمين ورجال الأعمال ذوو الدخل المرتفع، وحدد سقف السحب أو الدفع بواسطتها بـ: 100.000دج أسبوعيا.

الشكل رقم (III-3): البطاقة البنكية CIB

المصدر: www.bdl.dz تاريخ الاطلاع: 2023.07.10، الساعة: 14:10.

2- البطاقة البنكية فيزا La Carte VISA: هي بطاقة دولية تعمل للسحب والدفع والاطلاع على الحساب الإلكتروني لزبائن ذوي حسابين مفتوحة بالدينار الجزائري وبالعملة الأجنبية، تصدرها شركة فيزا العالمية (visa international) الأمريكية، تستعمل في أكثر من 200 دولة حول العالم، وتمكن من القيام بالعمليات مع أكثر من 32 مليون تاجر في العالم، 24/24سا وعلى مدار أيام الأسبوع، مدة صلاحيتها سنتين قابلة للتجديد بطريقة أوتوماتيكية، وتمكن هاته البطاقة بالاستفادة من خدمة التأمين على الحياة داخل الجزائر وخدمة تأمين السفر بالمجان إلى الخارج، ويوجد لها نوعين مختلفين هما كالآتي:

أ- بطاقة الفيزا الكلاسيكية: والتي تسمى بالفضية أيضا، حدد سقف السحب لهذه البطاقة فكان 500 أورو أسبوعيا.

ب- بطاقة الفيزا الذهبية: وتمسى أيضا Gold، سقف السحب بواسطتها هو: 5000 أورو في الأسبوع.

الشكل رقم (III–4): بطاقة فيزا الكلاسيكية وبطاقة فيزا الذهبية

المصدر: www.bdl.dz، تاريخ الاطلاع: 2023.07.10، الساعة: 15:10.

3–بطاقة ماستر كارد Master Card: هي بطاقة دولية تسمح القيام بكل عمليات التحويل والدفع، خدمة الدفع الإلكتروني وسحب الأموال في الخارج، عن طريق الإنترنت أو عن طريق آليات الدفع والسحب الإلكتروني 24سا/24سا على مدار أيام الأسبوع في كل بلدان العالم، وكذا الاطلاع على الرصيد عبر تلك الموزعات الالكترونية، مدة صلاحيتها سنتين قابلة للتجديد بطريقة أوتوماتيكية، وتمكن هاته البطاقة بالاستفادة من تأمين السفر بالمجان إلى الخارج، والشركة التي تصدرها هي MasterCard Worldwide الأمريكية، ويوجد لها نوعين مختلفين هما كالآتي:

أ- **Credit Card (البطاقة الائتمانية)**: هي بطاقة كلاسيكية أو فضية وتسمى (تيتانيوم)، توفر نوع من القروض إذ يقوم صاحب البطاقة بتسديد قيمة السحوبات التي يقوم بها دفعة واحدة شهريا، أو تأجيلها مع سداد قيمة الفائدة المترتبة على المبلغ، حيث حدد سقف التخليص بواسطتها بـ: 5000 أورو أسبوعيا، والسحب بـ: 1000دج أورو أسبوعيا.

ب- **Debit Card (بطاقة الخصم المباشر)**: هي بطاقة ذهبية تسمى (بلاتينيوم)، تعتمد الخصم المباشر من حساب العميل البنكي أو دفتر شيكاته دون الحاجة لإصدار فواتير، كما يمكن استخدامها للسداد عبر الانترنت وهي تقدم خدمة الطوارئ على مدار الساعة، وحدد سقف التخليص بواسطتها بـ: 8000 أورو أسبوعيا، والسحب بـ: 1500 أورو أسبوعيا.

الشكل رقم (III–5): بطاقة الماستر كارد

المصدر: www.bdl.dz، تاريخ الاطلاع: 2023.07.11، الساعة: 10:10.

4-البطاقة البنكية كوربورايت Corporate Card: هي بطاقة بنكية حديثة أطلقها بنك التنمية المحلية بالجزائر مؤخرا منذ بداية سنة 2019، حيث خصصت للمهنيين (أطباء، محامين، موثقين، رصاصين،...الخ) وكذا المؤسسات وتستعمل من أجل تخليص وتغطية مختلف النفقات المهنية والمتمثلة في مرافقة وتأمين تنقلات المتعاملين وتسهيل معالجة بيانات النفقات المهنية فهي تسهل عملية التحكم في الميزانية المخصصة للنفقات المهنية وهي تتطلب فتح حساب جاري وهي تمكن القيام بالعمليات عن طريق الانترنت 24سا/24سا، وكذا على مستوى موزعات الدفع الالكتروني أو أجهزة الدفع الالكتروني، وهي صالحة لمدة ثلاثة (03) سنوات قابلة للتجديد، كما لها نوعين هما: الكلاسيكية والذهبية كما يلي:

أ-بطاقة كوربورايت الفضية: حدد سقف السحب بواسطتها بـ: 50.000دج شهريا، أما الدفع بـ: 500.000دج شهريا، والدفع من خلال الإنترنت بسقف 80.000دج شهريا.

ب-بطاقة كوربورايت الذهبية: حدد سقف السحب بواسطتها بـ: 100.000دج شهريا، أما الدفع بـ: 900.000دج شهريا، والدفع من خلال الإنترنت بسقف 300.000دج شهريا.

الشكل رقم (III-6): بطاقة كوربورايت

المصدر: **www.bdl.dz، تاريخ الاطلاع: 2023.08.11، الساعة: 16:00.**

المطلب الثالث: السياسة الأمنية السيبرانية الخاصة بالمعاملات الإلكترونية على مستوى بنك BDL غرداية

لكل مؤسسة بنكية سياسة أمنية خاصة بها فيما يتعلق بالمعاملات الإلكترونية، أما بالنسبة لبنك التنمية المحلية بولاية غرداية محل دراستنا، فاستراتيجيته وسياسته الأمنية هي تشمل ما يلي:[1]

- **بالنسبة لمصدِر البطاقات والأجهزة المرتبطة بها:**

يعتمد بنك التنمية المحلية بشكل كبير على شركة النقد الآلي والعلاقات التلقائية بين البنوك (SATIM) Société Algérienne D'automatisation des Transaction Interbancaires et

[1] مقابلة مع السيد/ محمد فسيو، المنسق الجهوي لبطاقات الدفع الإلكترونية، بنك التنمية المحلية غرداية، بتاريخ: 04-06-2022، على الساعة: 09:00.

de Monétique)، هاته الأخيرة أنشأت سنة 1995 بمبادرة من ثمانية بنوك جزائرية وهي: (بنك التنمية المحلية، بنك الجزائر الخارجي، بنك الفلاحة والتنمية الريفية، البنك الوطني الجزائري، القرض الشعبي الجزائري، الصندوق الوطني للتوفير والاحتياط، صندوق التعاون الفلاحي، بنك البركة) وجاء هذا التجمع نتيجة استحالة قيام كل بنك بإنشاء مركزا خاصا به لتسيير ودراسة عمليات النقد الآلي الخاصة به، وذلك لأن العملية تتطلب استثمارات وتكاليف كبيرة على عاتق كل بنك، تضم الآن شبكة النقد الآلي لشركة النقد الآلي والعلاقات التلقائية بين البنوك 16 بنكا منها 07 بنوك عمومية و09 بنوك خاصة، إضافة إلى بريد الجزائر، حيث تتكفل شركة SATIM بإصدار البطاقات الإلكترونية وتطويرها وطبع الإشارة (الرمز) السري وكذا أيضا إصدار الموزعات والشبابيك الآلية بالإضافة إلى الربط بين تلك الموزعات الآلية للأوراق DAB أو الشباك الآلي البنكي GAB (Guichet Automatique de Bancaire) بواسطة شبكة اتصال خاصة تسمى SWIFT وكذا من خلال وضع الشبكة المالية بين البنوك المسماة (RMI)، وهذا من أجل السماح بعمليات الدفع والسحب والتحويل بواسطة البطاقات الإلكترونية CIB سواء كانت داخلية أو خارجية ما بين البنوك الأعضاء، أو حتى دفع مستحقات البضائع والخدمات لدى التجار المنخرطين في شبكة النقد الآلي بين البنوك من خلال نهائيات الدفع الإلكتروني (Terminal de Paiement Electronique) (TPE)، ومن مهامها أيضا تأمين قبول البطاقة في جميع المصارف المشاركة وإجراء عمليات المقاصة لصفقات السحب بين المصارف وتأمين تبادل التدفقات المالية بين البنوك المشاركة والمؤسسات، بالإضافة إلى مراقبة البطاقات المزورة وكشف كل التلاعبات، بحسب المقاييس المعمول بها دوليا.

➢ **بالنسبة للشبكات الاتصالية:**

يعتمد بنك التنمية المحلية BDL على شبكة اتصالية إلكترونية تسمى SWIFT منذ أن تم ربطه بها سنة 1991م فهي شبكة مهامها الاتصال وتحويل البيانات الحزمية باستعمال معيار الآيتيو X25 للاتحاد العالمي للاتصالات السلكية واللاسلكية، وهي تسمح بربط الأجهزة والشبكات الاتصالية، حيث تتمثل مجالات استخدام هذه الشبكة في مختلف أصناف البرامج المستخدمة في الاتصالات بين وكالات البنك مع التحويلات المالية والعمليات البنكية من خلال نظام واحد بين البنوك ولغة واحدة بالاعتماد على نظم تشفير إلكترونية **لتحقق بذلك كل من بعد سرية البيانات، التوافر والديمومة، احترام الخصوصية، التكنولوجيا المستخدمة.**

يوجد بالبنك شبكة محلية (الأنترانت) (LAN): تربط بين الخادم وأجهزة الكمبيوتر الخاصة بالبنك وتأخذ هذه الشبكة الهيكلة السلسة (الخطي) ويرجع السبب وراء اختيار هذا النوع من الهيكلة هو أنه في حالة توقف أحد الأجهزة لا تتعطل الشبكة **(بذلك تحقق بعد التوافر والديمومة)**، بالإضافة الى انها تتميز بسهولة إدارتها وإضافة أو سحب حواسيب من الشبكة وترتبط الشبكة المحلية مع جميع الشبكات المحلية لبنوك التنمية المحلية على مستوى التراب الوطني لتكوين شبكة واسعة.

بالنسبة للشبكة الخارجية لبنك التنمية المحلية (الإكسترانت): فهي تمتلك من نوع التوزيع بحيث يمكن لأي زبون يملك حساب لدى البنك أن يدخل موقع البنك ويطلع على بعض الصفحات عن طريق كلمة السر الممنوحة له، ولضمان العمل الجيد للشبكة يتخذ البنك احتياطات أمنية تتمثل في برامج مضادة للفيروسات Antivirus.

أما بخصوص الإنترنت: فالبنك يشترك بالشبكة العالمية للإنترنت من نوع ADSL بسرعة 256 KBS، ف ISP (Internet Service Provider) هو مزود خدمة الإنترنت من احدى الشركات الأعضاء CIX.

أما بالنسبة للشبكة النقدية المشتركة RMI: بنك التنمية المحلية ضمن البنوك التي المستخدمة للنظام النقدي المشترك ما بين البنوك الذي يستخدم الشبكة النقدية المشتركة والتي تتضمن حظيرة الموزعات الآلية للأوراق النقدية DAB الموزعة على كامل الوكالات البنكية والبريدية المستعملة لشبكة نقل: DZ-PAC، حيث تقوم هذه الموزعات بمعالجة عمليات السحب المرتبطة بالبنوك الأعضاء وكذا التحويلات المالية المرتبطة بعمليات المقاصة الناتجة عن السحب.

بالنسبة للهاتف النقال: لا تزل الخدمات المقدمة من طرف البنوك الجزائرية لزبائنها عبر الهاتف المحمول تقتصر على الاطلاع على الأرصدة وطلب الصكوك، وكذا تحويل الأموال من رصيد إلى رصيد آخر داخل وكالات البنك، إضافة إلى إمكانية دفع الفواتير الخاصة بالمتعامل، لذا يمكن القول أن البنوك الجزائرية لا تستخدم الهاتف المحمول في تقديم خدماتها رغم تطوره واتشاره على كافة التراب الوطني، وعليها الاستفادة من عدد مشتركي خدمة الهاتف النقال في تقديم خدماتها لجلب أكبر عدد من العملاء.

- **بالنسبة للبرمجيات وأنظمة المعلومات:**

البرمجيات وأنظمة المعلومات المعتمدة من قبل بنك التنمية المحلية هي خاصة بشركة الجزائر لخدمات الصيرفة الإلكترونية (AEBS) التي توفر برمجيات وأنظمة معلومات متطورة لمختلف الخدمات المالية المصرفية وتأمين التبادل الإلكتروني للبيانات خاصة الخدمات التي تعتمد على شبكة الإنترنت والفضاء السيبراني (**لتحقيق بعدي سرية البيانات واحترام الخصوصية**)، بالرغم من أن الخدمات المقدمة عبر الإنترنت من قبل المصارف في الجزائر هي حاليا بسيطة وقليلة تحتاج إلى توزيع وشركة AEBS تعتبر بحق أول خطوة للجزائر في مجال الصيرفة الإلكترونية.

ومن الأنظمة المعتمدة من قبل بنك التنمية المحلية في المعالجة الآلية لعمليات السحب والدفع بالبطاقات البنكية وكذا معالجة عمليات المقاصة:

- **أنظمة الدفع الإلكترونية:**

يعتمد بنك BDL على شركة الجزائر لخدمات الصيرفة الإلكترونية (EDI) التي أنشأت سنة 2004 بشراكة بين المجموعة الفرنسية DIAGRAM EDI الرائدة في مجال برمجيات أنظمة الدفع المتعلقة بالصيرفة

الإلكترونية وأمن تبادل البيانات المالية وثلاث مؤسسات جزائرية هي: (AGACT MULTIMEDIA) و(SOFT ANGINERING) ومركز البحث في الإعلام العلمي والتقني (CERIST)، ومن مهام شركة EDI التركيز على عمليات تطوير وتدعيم وعصرنة الخدمات البنكية وأنظمة الدفع الإلكترونية، حيث تقدم هذه الشكات خدماتها المتعلقة بالمصارف عن بعد وتسيير وأمن تبادل البيانات الآلية لجميع البنوك والمؤسسات المالية باختلاف أصناف زبائنها (مؤسسات كبرى، مجموعة شركات، تجار، مهنيين، خواص...) وتقديم تشكيلة من الخدمات بدرجة عالية من الأمن وسلامة في الأداء.

-**يستخدم البنك نظام ARTS** (**Algeria Real Time Settlements**): الذي يعد من بين أنظمة الدفع التي تعتمد عليها البنوك الجزائرية، وهو نظام دفع حديث، كما أنه يهدف إلى تحسين الخدمات الإلكترونية المصرفية خاصة من حيث أنظمة الدفع وذلك لمواكبة المعايير الدولية، ويرمز إليه أيضا بـ: (RTGS Real Time Gross Sottement System) بمعنى نظام التسوية الإجمالية الفورية أي نظام الدفع الفوري للمبالغ المالية الكبيرة هو نظام تسوية المبالغ الاجمالية بين البنوك في وقت حقيقي ويتم فيه سير التحويلات بصفة مستمرة وعلى الفور بدون تأخير أو تأجيل وعلى أساس إجمالي (**التوافر والديمومة**).

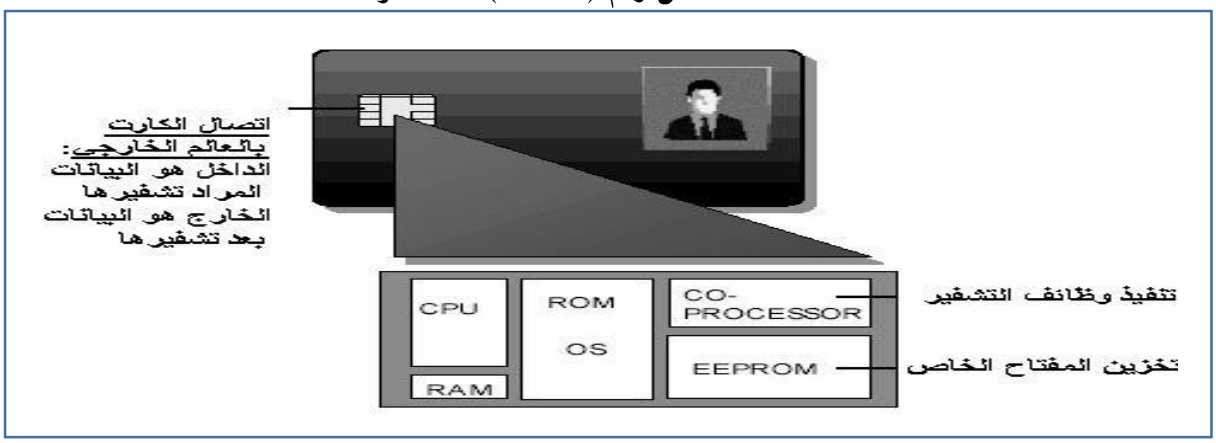
-**كما يستخدم بنك نظام المقاصة الإلكترونية للمدفوعات** (**ATCI**) : هذا النظام هو مكمل لنظام RTGS حيث يختص بالمعالجة الآلية لوسائل الدفع العام Les Instruments de Paiement de Masse، صكوك ، تحويل مالي، اقتطاع، عمليات السحب والدفع بالبطاقات البنكية، وذلك باستعمال وسائل متطورة مثل الماسحات الضوئية (Scanners) والبرمجيات المختلفة، ويمثل هذا النظام القسم الثاني من أنظمة الدفع المتطورة، ووفق المعايير الدولية، بهدف التحسين النهائي للخدمات البنكية المقدمة للعملاء، حيث تتم عملية المقاصة بصورة آلية بين البنوك بالاعتماد على الربط الشبكي فيما بينها.

- **بالنسبة للتشفير:**

في البداية اعتمد البنك على نظام التشفير باستخدام المفاتيح العامة يدعى بنظام RSA وهذا النظام يعتبر أبطأ مقارنة مع نظام التشفير المتماثل فهو أكثر أمانا لكنه ليس عصيا على الاختراق، لذلك تم تطوير نظام PGP وهو نظام محسن لـ RSA، ونظام PGP لا يزال منيعا على الاختراق حتى يومنا هذا فهو يستخدم مفتاح بطول 128 Bits إضافة إلى استخدامه البصمة الإلكترونية للرسالة. لذلك اتفقت شركتا ماستر كارد وفيزا كارد على تقنيات فنية مشتركة (التشفير) لحماية التسويق الذي يتم عبر شبكة الإنترنت باستعمال بطاقات الائتمان الممغنطة Credit Cards، بغية تحقيق سرية البيانات.[1]

[1] هيثم المسيري، **ندوة الخدمات البنكية الإلكترونية الشاملة (رؤية مستقبلية)**، كتاب أعمال الملتقى العربي الأول حول المصارف الإسلامية، الواقع والتحديات، المنعقد يومي: 25-29 نوفمبر 2007، الشارقة، الإمارات العربية المتحدة، نشر عن المنظمة العربية للتنمية الإدارية، القاهرة، مصر، 2011، ص 22.

الشكل رقم (III–7): التشفير



المصدر: هيثم المسيري، ندوة الخدمات البنكية الإلكترونية الشاملة (رؤية مستقبلية)، كتاب أعمال الملتقى العربي الأول حول المصارف الإسلامية، الواقع والتحديات، المنعقد يومي: 25–29 نوفمبر 2007، الشارقة، الإمارات العربية المتحدة، نشر عن المنظمة العربية للتنمية الإدارية، القاهرة، مصر، 2011، ص 22.

- **بالنسبة للتوقيع الرقمي:**

يجعل التوقيع الرقمي تحويل المعاملات أكثر أمنا وسرية فهو بمثابة ختم الهوية التي تلازم الرسالة عبر الإنترنت، فبنك التنمية المحلية يستخدمه من أجل التأكد من أن الرسالة قد جاءت من مصدرها دون التعرض لأي تغيير أثناء عملية النقل، بحيث يستخدم المرسل المفتاح الخاص لتوقيع الوثيقة إلكترونيا، أما المستقبل فيتحقق من صحة التوقيع عن طريق المفتاح العام بحيث تموه الرسالة أولا لإنشاء بصمة إلكترونية ثم تشفر البصمة الإلكترونية باستخدام المفتاح الخاص للمالك مما ينتج عنه توقيع رقمي يلحق بالوثيقة المرسلة وللتأكد من صحة التوقيع يستخدم المستقبل المفتاح العام المناسب لفك شيفرة التوقيع.

شكل رقم (III–8): التوقيع الرقمي

المصدر: المرجع السابق نفسه، ص 18.

➢ **بالنسبة للبصمة الرقمية:**

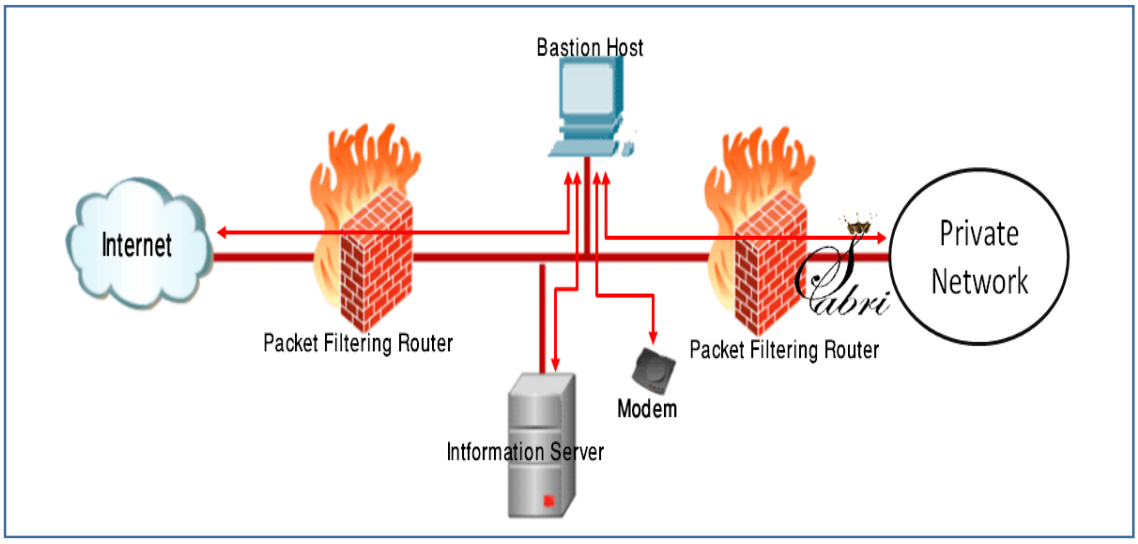
يعتمد بنك التنمية على بصمة رقمية متكونة من بيانات لها طول ثابت ما بين (128 و160 bits) حيث تؤخذ من الرسالة المحولة ذات الطول المتغير وهذه البصمة تميز الرسالة الأصلية والتعرف عليها بدقة، حيث إذا تم التغيير ولو بمقدار Bits في الرسالة هذا يؤدي إلى بصمة أخرى مختلفة تماما، حيث أن هاته البصمة الرقمية يتم اشتقاقها وفق خوارزميات معينة تدعى دوال أو اقترانات التمويه وتقوم هاته الخوارزميات بتطبيق حسابات رياضية على الرسالة لتوليد بصمة (رسالة صغيرة) تمثل ملف كامل أو رسالة (سلسلة كبيرة).

تتميز البصمات عن بعضها البعض بحسب المفاتيح الخاصة التي أنشأتها والتي لا يمكن فك شيفرتها إلا باستخدام المفتاح العام.

➢ **بالنسبة لجدار النار:**

يستخدم بنك BDL الجدار الناري لمراقبة جميع البيانات والمعطيات التي تصل إلى الخادم عبر الإنترنت، فهو برنامج تطبيقي يقوم بحماية البيانات المخزنة على الخادم من أي هجوم أو اختراق، وما أفادنا به المكلف بخلية الإعلام الآلي بالوكالة أن حواسيب البنك متصلة بالإنترنت مما يتوجب استخدام جدار ناري لأجل الحماية، وأنه في حالة تعليمات أو أوامر غير مسموح بها يعلم هذا البرنامج المستخدم عن حدوث اختراق للمعلومات كذلك في حالة دخول المستخدم إلى بيانات أو معطيات عبر الإنترنت فإن هذا البرنامج ينذر المستخدم بأن هذه المعطيات أو هذا الموقع غير آمن.

الشكل رقم (III-9): عمل جدار النار



المصدر: https://www.frameip.com/firewall، تاريخ الاطلاع: 23-08-2023، على الساعة: 10:20.

➢ **بالنسبة للموجهات (الراوتر):**

موجه للخدمات المدمجة (Integrated Services Router ISR)، وظيفته كموجه كتصفية المرور الشبكي، والقدرة على تشغيل نظام حجب الدخلاء (Intrusion Prevention System IPS)، والتشفير، وتشغيل الشبكة الافتراضية الخاصة VPN (Virtual Private Network)، والتي تتيح اتصال مشفر بتقنية نفق البيانات Tunneling.

الشكل رقم (III–10): الموجهات (الراوتر)

المصدر: https://www.sans.org/about، تاريخ الاطلاع:23–08–2023، على الساعة: 11:30.

➢ **أجهزة منع الدخلاء (IDS): Intrusion Detection System.**

هو نظام اكتشاف الدخلاء على شكل جهاز شبكي يقوم بمسح البيانات ومقارنتها بقاعدة بيانات كبيرة تحتوي على قواعد منطقية أو بصمات للهجمات السابقة، ويقوم بعملية المسح لاكتشاف المرور الشبكي الخبيث، فإذا وجد تطابق يقوم مكتشف الدخلاء بتسجيل الاكتشاف ويرسل إنذار لمشرف الشبكة **بمعنى يتتبع الأثر**، فهو لا يقوم بردع الهجمات ولا يقوم بمنع حدوث الهجمات ولكن وظيفته الوحيدة هي فقط اكتشاف ذلك وتسجيلها وإطلاق إنذار عند حدوثها. عملية مسح البيانات تقوم بإبطاء سرعة التدفق في الشبكة ويعرف هذا الإبطاء بوقت الاستجابة Latency، ولمنع بطئ التدفق الشبكي يتم وضع مكتشف الدخلاء بعيدا عن المسار المروري للشبكة ليفحصها منعزلا.

الشكل رقم (III–11): أجهزة منع الدخلاء (IDS)

المصدر: https://www.sans.org/about، تاريخ الاطلاع: 23–08–2023، على الساعة: 13:30.

➢ **بالنسبة لبرتوكولات الحركات المالية الآمنة SET:**

برتوكولات الحركات المالية الآمنة: SET: Secure Electronic Transaction والذي أدخلته كل من VISA International وMaster Card اذ يتيح معرفة أطراف التبادل والتحقق من هوية الآخر من خلال تبادل التوقيعات الإلكترونية، حتى أنه أضحى بمثابة الحكم في أغلب عمليات الدفع التي تجري عبر الإنترنت، غير أن الاستفادة من مزايا هذا النظام تقتضي وصل قارئ بطاقات un lecteur de carte à puce بجهاز الكمبيوتر.

أطلق على هذا البرتوكول اسم برتوكول الحركات المالية الآمنة والغاية من هذا الحفاظ على أمن البيانات أثناء إجراء الحركات المالية عبر شبكة الإنترنت، ويعتمد هذا النظام على برمجيات تدعى برمجيات المحفظة الإلكترونية التي بدورها تعتمد على قيام هيئة الاعتماد Certificate Autority على إنشاء وحدة استخراج هويات إلكترونية Certificate، لكل من العميل التاجر على أن يستخرج هذه الهويات بطريقة مضمونة مؤمنة وسرية، ويعد نظام تأمين المعاملات الإلكترونية SET من أبرز وأقوى الأنظمة التأمينية الموثوق بها في حالة المعاملات الإلكترونية، وخصوصا عملية الوفاء الإلكتروني عبر شبكة الإنترنت أو ما يسمى بالوفاء عبر الخط، وهو يعتمد على بروتوكولات تأمينية مركبة، تم تطويرها من قبل شركة فيزا كارد Visa Card وماستر كارد Master Card.

إن إجراء برتوكول الحركات المالية يشترط وجود بطاقة بنكية يستعملها العميل الإلكتروني في شراء سلع وخدمات مختلفة، ويعتبر هذا البرتوكول من البرامج الأكثر أمانا، وذلك استنادا إلى التشفير والتوقيعات الرقمية.[1]

فبنك التنمية المحلية يسمح لعملائه القيام بالمعاملات المالية من خلال الدخول إلى الصفحة الإلكترونية عبر الإنترنت، فتسمح هاته الخدمة للعملاء الذين لديهم البطاقات الإلكترونية الممولة برقمها السري، وعند إجراء الحركات المالية ما بين الزبون والتاجر فإنه لا يمكن مشاهدة رقم البطاقة الائتمانية لهذا الزبون باستخدام هذا البرتوكول حيث ترسل الصيغ المشفرة لهذا الرقم إلى مصدر البطاقة للموافقة على إجراء الحركة المالية مع التاجر، كما يمكن للتاجر تلقي الدفعات من الزبائن دون شهادة برتوكول SET وما على التاجر إلا استخدام شهادة SET الخاصة به لتوثيق الحركات المالية مع البنك ومعالج الحركات المالية لأي طرف آخر يتعامل معه، وهذا ما يعزز الثقة والحماية والأمان في صحة التعاملات المالية وقبولها ومن هنا يولد التاجر السند ويرسل البضاعة.

➢ **بالنسبة لبرتوكولات الطبقات الأمنية SSL:**

SSL هي اختصار للكلمة الإنجليزية: Secure Sockets Layer، برنامج من أنواع التكنولوجيات المستعملة في تشفير مجموعة من العمليات التي تنتقل عبر الإنترنت، به برتوكول تشفير متخصص لنقل البيانات

[1] مصطفى كافي، **النقود والبنوك الإلكترونية**، دار رسلان، دمشق، سوريا، 2012، ص 213.

والمعلومات المشفرة بين جهازين، عبر شبكة الإنترنت بطريقة آمنة، ولا يمكن قراءتها إلا من طرف المرسل والمستقبل، لأن قوة تشفيرها قوية ويصعب فكها وهي تختلف عن طرف التشفير الأخرى في أمر واحد وهو أنه لا يطلب من المرسل البيانات تشفير المعلومات التي يريد حمايتها فقط عليه التأكد من أن البرتوكول مستخدم بالقوة المطلوبة، كما طورت هذه التقنية من قبل شركة نت سكيب التي تساعد في **زيادة الثقة في التجارة الإلكترونية ومستوى الأمان بمستوى عال من السرية وقدرتها على تتبع أثر مختلف العمليات**، وسميت بهذا باسم الطبقات الآمنة لأنها تعمل كطبقة وسيطة بين البروتوكولات، وينقسم SSL إلى قسمين: برتوكول الطبقات الأمنية بدون وسيط وبرتوكول الطبقات الأمنية بوسيط.

أ– برتوكول الطبقات الأمنية بدون وسيط: هو نظام مقيس Normalisé بواسطة الإنترنت Engineering task force تحت اسم Transport Layer Security (TLS)يسمح بنقل رقم البطاقات البنكية على الإنترنت بشكل آمن برتوكول الطبقات الأمنية SSL اليوم هو النظام الأكثر استخداما على الإنترنت.

ب–برتوكول الطبقات الأمنية بوسيط: يقوم التاجر باستدعاء وسيط، ويقوم موفر الأمان بتنفيذ برتوكول على Serveur Marchand، وتوزيع الشهادة الإلكترونية على التاجر الإلكتروني (الذي تم شراءه) من جهة خارجية موثوق بها، وتوفير الصيانة بشكل عام، تكون التعريفة ذات الحدين تتكون من تعريفة ثانية على كل معاملة أو تعريفة متغيرة في شكل عمولة، وفي وضع SSL بوسيط يوجد فقط عدم تماثل واحد بين التاجر الإلكتروني (المورد الإلكتروني) ومستخدم الإنترنت، وهناك كذلك ما يسمى بـ EMV* (Euro Master Card Visa)، حيث يحدد برتوكول معاملة الدفع، بناء على استخدام البطاقة الذكية، آمنة وقابلة للتشغيل المتبادل دوليا. وأقسامه تسمح بالاقتراب من EMV من زاويتين رئيسيتين، وهما الجوانب المتعلقة بالمعاملات والأمان للبرتوكول،[1] فمثلا أرغمت السلطات العمومية البنوك على اعتماد النظام المالي العالمي EMV والتي تعتبر نقطة إيجابية إذا علمنا أن البلدان الأوروبية لم تعتمد هذا النظام إلا بعد 30 سنة من إصدار أولى بطاقات الائتمان، فمسؤولية السلطات والبنوك في هذا التأخر.

ففي البنك يقوم هذا البرنامج بربط المتصفح الموجود على جهاز العميل (المستخدم أو المشتري) بجهاز الخادم الخاص بالموقع المراد الشراء منه وهذا طبعا إذا كان مزودا لهذه التقنية أساسا ويقوم هذا البرنامج بتشفير أي معلومة صادرة عن ذلك المتصفح وصولا إلى جهاز الخادم باستخدام برتوكول الإنترنت TCP/IP **(تحقيق السرية التامة)**.

(*): EMV: عبارة عن معيار تقني للمعاملات التي يتم مباشرتها عبر بطاقات السحب والائتمان.

[1] Vincent Alimi, **Contributions au Déploiement des Services Mobiles et a L'analyse de la Sécurité des Transactions**, Thèse présentée en vue de l'obtention du doctorat en informatique et applications, université de Caen – basse Normandie, 2012, P 96.

مثلا: عند دخول زائر (المشتري) الموقع للصفحة الآمنة التي يدخل فيها البيانات والمعلومات للشراء يقوم المتصفح بهذا البرنامج بالجهاز الخادم الأمن للموقع الذي يطلب منه: رقم بطاقة الائتمان ورقمها السري للتأكد من مصداقية الموقع، علما أن هذه الخطوات تتم بواسطة المتصفح دون علمه أو تدخله، وبعد التأكد يقوم المتصفح بإعلامه بالتطابق أو عدمه (**بمعنى له القدرة العالية في تتبع الأثر**).

- **بالنسبة لاستخدام تقنية الفتحات الآمنة SLL:**

يستخدم البنك هاته التقنية لزيادة الثقة في المعاملات الإلكترونية بمختلف أنواعها لما توفره من مستوى الأمان والتي طورتها شركة "نت سكيب" مما جعلتها أساس المعاملات الإلكترونية في العالم وأصبحت ضرورية، فبرنامج SLL هو برنامج يحتوي على برتوكول تشفير متخصص TCP/IP لنقل البيانات والمعلومات المشفرة بين جهازين عبر شبكة الإنترنت بطريقة آمنة بحيث لا يمكن قراءتها إلا من طرف المرسل والمستقبل لأن قوة تشفيرها قوية ويصعب فكها وهي تختلف عن طرق التشفير الأخرى.[1]

فبنك التنمية المحلية يسمح لعملائه القيام بالمعاملات المالية من خلال الدخول إلى الصفحة الإلكترونية عبر الإنترنت، حيث تسمح هاته الخدمة للعملاء الذين لديهم البطاقات الإلكترونية من الدخول لمعلوماتهم المصرفية من أي مكان وعلى مدار الساعة سواء في المنزل أم المكتب، وذلك بأن يفتح العميل الموقع الإلكتروني للبنك ويدخل الموقع المخصص للخدمة المصرفية ثم يدخل رقم البطاقة والرقم السري، كما أنه يتم إعطاء رقم شخصي تعريفي له PIN لتسهيل الدخول وإجراء المعاملات المالية وبالتالي يمكن للعملاء التحكم بأموالهم مع توافر إجراءات حماية وأمان في عملية التصفح والبحث وكذلك إمكانية الطباعة لأي معاملة وأحيانا تصميم صفحة خاصة بالحسابات بالشكل الذي يختاره العميل والأسهل له في التصفح.

- **النسخ الاحتياطي**: يقوم البنك كإجراء من إجراءات الحماية بتجهيز نسخ احتياطية لجميع البيانات والمعطيات الخاصة بنظم المعلومات وكافة العمليات التشغيلية، من مثل حسابات المستخدمين وكلمات المرور الخاصة بهم وبريدهم الإلكتروني والبيانات المخزنة على إحدى وسائط التخزين سواء داخل النظام أو خارجه وفقا لجدول زمني معين، وذلك لضمان عدم فقدان البيانات بسبب أي خلل أو هجوم خبيث.

المبحث الثاني: تصميم أداة الدراسة وأساليب جمع ومعالجة البيانات

اعتمدت الدراسة في جمع البيانات على أداة الاستبانة، وذلك بهدف استطلاع توجه عينة المجتمع، حيث يجب تصميمها استنادا على عدد من الأدبيات والدراسات السابقة المتاحة كما يلي:

[1] كريمة صراع، **واقع وآفاق التجارة الإلكترونية في الجزائر**، رسالة ماجستير، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، المدرسة الدكتورالية للاقتصاد وإدارة الأعمال، وهران، الجزائر، 2014، ص 79-83.

المطلب الأول: الأدوات والأساليب الإحصائية المستخدمة في الدراسة

أولا: أداة الدراسة:

تقوم هذه الدراسة على المنهج الوصفي، حيث اعتمدنا على أداة "**الاستبانة**" لتجميع البيانات، ومنه قمنا بتصميم الاستبانة على ضوء أهداف الدراسة وتساؤلاتها، فقمنا بتصميم استمارة مكونة من (46) عبارة بطرح مجموعة من الأسئلة متعلقة بالبيانات العامة الخاصة بالمستجيب وأسئلة تتعلق بأبعاد الأمن السيبراني للبنك وأسئلة أخرى عن ثقة العملاء ثم أسئلة عن الخدمات الإلكترونية المصرفية.

ثانيا: الأساليب الإحصائية المستخدمة في الدراسة:

تم استخدام الإحصاء الوصفي والتحليلي لوصف متغيرات الدراسة المتعلقة بالخصائص الديمغرافية وتحليل المتغيرات التابع ووسيط والمستقل والعلاقة الإحصائية لإثبات صحة الفروض والإجابة على الإشكالات المنهجية المطروحة في متن الدراسة من خلال البرنامج الإحصائي للعلوم الاجتماعية Spss v26 وبرنامج Excel من أجل تصميم الأشكال البيانية، وكذا برنامج Smart PLS.4 المستخدم في الاختبار، وتم الاعتماد على بعض الأساليب الإحصائية كما يلي:

1.معامل ارتباط بيرسون: يستخدم لقياس اتجاه وقوة العلاقة بين المتغيرات وإيجاد ارتباط الفقرات بالدرجة الكلية للبعد الذي تنتمي إليه، وهذا لتقدير الاتساق الداخلي، وتم استخدامه في في حساب صدق الاستبيان واختبار فرضيات الدراسة.

2.استخدام معامل ألفا كرومباخ: لقياس ثبات أداة الدراسة، وإن كانت معادلة ألفا كرومباخ لا تعد من الأساليب الإحصائية الخالية من براثن التلوث الإحصائي[1].

3.مقاييس الإحصاء الوصفي: للتعرف على البيانات الأولية لمفردات الدراسة، ولتحديد آراء الأفراد تجاه عبارات الأبعاد التي تضمنتها أداة الدراسة فقد تمت الاستعانة بأهمها مثل: الوسط الحسابي التكرارات والنسب المئوية: وذلك لحساب متوسطات فقرات الاستبيان وكذا الانحراف المعياري كونه القيمة الأكثر استخداما من بين مقاييس التشتت الإحصائي لقياس مدى التبعثر الإحصائي، أي أنه يدل على مدى امتداد مجالات القيم ضمن مجموعة نتائج الاستبيان: **المتوسط الحسابي:** وهو متوسط مجموع القيم المدروسة مقسوم على عددها يستخدم بغية التعرف على متوسط إجابات المبحوثين حول الاستبيان ومقارنتها بالمتوسط الفرضي المقدر بـ: (03) لأن التنقيط يتراوح من (01) إلى (05)، والمتوسط يساعد في ترتيب العبارات حسب أعلى قيمة له.

[1] محمد بوزيان تيغزة، **توجهات حديثة في تقدير صدق وثبات درجات أدوات القياس**، مجلة العلوم النفسية والتربوية، جامعة الشهيد حمة لخضر، الوادي الجزائر، المجلد 04 العدد 01، مارس 2017، ص ص 10-11.

4.الانحراف المعياري: استخدم من أجل التعرف على مدى انحراف استجابات المبحوثين اتجاه كل فقرة وبعد، وللتأكد من صلاحية النموذج لاختبار الفرضيات، ويوضح التشتت في استجابات أفراد العينة، فكلما اقتربت قيمته من (0) فهذا يعني تركز الإجابات وعدم تشتتها، وبالتالي تكون النتائج أكثر مصداقية وجودة، كما يفيد في ترتيب العبارات لصالح أقل تشتتا عند تساوي المتوسط الحسابي المرجح بينها.

5.النمذجة بالمعادلة الهيكلية SEM (Structural Equation Modeling): تعتبر النمذجة بالمعادلة الهيكلية تقنية إحصائية متقدمة، حيث تقدم عدد من الإجراءات التي تساعد في تفسير العلاقات بين متغيرات الظاهرة المدروسة، ويندرج فيها مجموعة من الأساليب الإحصائية المتنوعة مثل تحليل الانحدار الخطي المتعدد، التحليل العاملي التوكيدي والاستكشافي، تحليل المسار للمتغيرات الظاهرة والكامنة، تحليل التسلسل الزمني، كما أنها تتيح للباحثين تقدير مساهمة المتغير في بناء المفهوم أو النظرية، كما يتيح هذا الأسلوب بكفاءة إمكانية اختبار النماذج النظرية من خلال تحري وفحص العلاقات بين مجموعة من المتغيرات، ثم تفسير وتحليل العلاقات بين المتغيرات العديدة أو المعقدة.[1]

خصائص النمذجة الهيكلية SEM:

يمثل هذا الأسلوب أو التقنية انعكاسا لثلاثة أفكار تمثل خصائص رئيسية في تحليل البيانات الإحصائية الحديثة وهي:

- يستخدم مصطلح نموذج لتمثيل نظرية تفترض علاقات بين متغيرات الدراسة.
- يعني مصطلح المعادلة أن التعبير عن مختلف العلاقات بين المتغيرات يتم باستعمال قواعد الجبر الصريحة.
- يستخدم مصطلح الهيكلة للإشارة إلى أن المعادلات الجبرية تمثل مسارا محددا مبني على أساس البيانات الحقيقية التي توافق النموذج ومن ثم النظرية.
- إمكانية دراسة تأثير المتغير الوسيط بين المتغيرات التابعة والمستقلة في نموذج الدراسة.
- أمكانية تعديل النموذج المفترض وفقا للحاجة العلمية لذلك.

متغيرات النمذجة بالمعادلات الهيكلية:

تتمثل متغيرات النمذجة بالمعادلات الهيكلية في المتغيرات الظاهرة (المؤشرات) والكامنة (المتغيرات) وهي:

-المتغيرات الظاهرة (Manifest Variables):

هي مجموعة من المتغيرات التي تستخدم لتحديد أو الاستدلال على البنية أو المتغير الكامن، وهي المتغيرات التي يمكن قياسها حيث تتمثل المتغيرات الظاهرة في المؤشرات (Indicators) الخارجية للمتغيرات الكامنة،

[1] Byrne k, **How do Consumers Evaluate Risk in Financial Products**, Journal of Finance Services Marketing, Vol 10, N 1, 2010, p 03.

ويطلق عليها عدة مسميات مثل المتغيرات المشاهدة أو الملاحظة (Observed) أو المقاسة (Measurable).

-المتغيرات الكامنة (Latent Variables):

هي المتغيرات (Constructs) النظرية أو الافتراضية لا يمكن ملاحظتها بصورة مباشرة، أو هي المتغيرات غير المقاسة (Unmeasured) أو العوامل أو المتغيرات غير المشاهدة أو المباني الافتراضية، بمعنى آخر هي المتغيرات التي لا يتم مشاهدتها أو قياسها مباشرة، ولكن يمكن ملاحظتها وقياسها بشكل غير مباشر، حيث يستدل عليها بواسطة مجموعة من المؤشرات التي يتم اعدادها لقياسها باستخدام الاختبارات والاستبيانات وغيرها من أدوات جمع البيانات. وعليه فإن المتغيرات الكامنة هي مباني أو تكوينات (Constructs) غير مشاهدة أو غير ملاحظة (Unobserved) فهي بمثابة التكوينات الفرضية (Hypothetical Constructs) أو العوامل (Factors) التي يستدل عليها من مؤشراتها الخارجية الظاهرة.

وتنقسم المتغيرات الكامنة إلى نوعين، متغيرات كامنة خارجية (Exogenous Latent Variables)، وهي المباني التي تفسر التركيبات الأخرى في النموذج، والمتغيرات الكامنة الداخلية (Endogenous Latent Variables) وهي تلك المباني التي يتم تفسيرها ضمن النموذج، يمكن توضيح أنواع المتغيرات وفق نمذجة (SEM).[1]

نموذج التحليل الاحصائي المقترح للدراسة: بالنظر إلى النتائج الأولية ومن أجل تحقيق مخرجات نتائج ذات جودة تحاكي التطورات الحاصلة في الأساليب والبرامج الإحصائية، تقرر اختيار أسلوب النمذجة بالمعادلة الهيكلية (SEM) بطريقة المربعات الصغرى الجزئية (PLS) مع البرنامج الاحصائي Smart PLS الحاسوبي الذي يشغل اختصارا نمذجة (PLS-SEM).[2]

البرنامج الاحصائي المتقدم (Smart PLS): صمم خصيصا لتنفيذ التحليل بطريقة المربعات الصغرى الجزئية (PLS) والمشغل بنظام (JavaEclipse)، كما يعد البرنامج من بين أشهر البرامج إلى جانب (R) و(PLSpm)، يتم تحديد نموذج تحليل المسار عن طريق السحب والاسقاط لتخصيص المؤشرات للمتغيرات الكامنة بغرض رسم النموذج الهيكلي، كما تجلب المدخلات من خلال تحميل ملفات البيانات من تنسيقات مختلفة، وبعد تكون النموذج الهيكلي يرافقه إضافة تنسيقات وبمخرجات أكثر دقة وتفصيل في نصوص عادية أو مع صفحة واب واستصدار نموذج هيكلي إلى صورة، علاوة على خيارات دعم التفاعلات والتأثيرات.[3]

---

[1] آسية بن أحمد، **أثر المرونة الإستراتيجية على جودة فاعلية الأداء وتنافسية المؤسسة، دراسة تطبيقية على شركة الاتصالات موبيليس**، أطروحة دكتوراه علوم تجارية، جامعة الجيلالي اليابس سيدي بلعباس، كلية العلوم الاقتصادية التجارية وعلوم التسيير، 2017، ص 212.

[2] Nesselroade McArdle, **Longitudinal Data Analysis Using Structural Equation Models 1ed**, Washington USA: American Psychological Association, 2014, p 28.

[3] الشيخ ساوس ومحمد فودو، **نمذجة المعادلات الهيكلية باستخدام المربعات الصغرى الجزئية مثال تطبيقي باستخدام R في بحوث المحاسبة والتدقيق**، مجلة معهد العلوم الاقتصادية، المجلد 22، عدد 01، 2019، ص ص 179-196.

أسباب اختيارنا لبرنامج Smart PLS مقارنة ببرنامج AMOS:

على ضوء ما سبق، أهم أسباب اختيارنا برنامج Smart PLS مقارنة ببرنامج AMOS كانت كما يلي:[1]

- ✓ معالجة العينات الصغيرة لا يطرح أي إشكال مع برنامجSmart PLS بخلاف برنامج AMOS فهو يتعامل مع العينات الكبيرة.
- ✓ يتميز برنامج Smart PLS بالمنهج الاستكشافي، بخلاف برنامج AMOS الذي يطبق فقط في حالة النماذج المبنية على نظريات قوية.
- ✓ يعتمد برنامج Smart PLS على المربعات الجزئية الصغرى (التباين/ الانحدار)، في حين برنامج AMOS يعتمد على التباين.
- ✓ يعالج البرنامج نماذج معقدة جدا بعدة متغيرات مستقلة وسيطية وتابعة.
- ✓ لا يشترط هذا البرنامج اعتدالية توزيع البيانات، لكون النمذجة بالمعادلات الهيكلية بطريقة المربعات الصغرى الجزئية هي طريقة غير معلمية.
- ✓ البرنامج يشترط أن تكون القيم المفقودة لا تتعدى المستوى المقبول.
- ✓ لا تتطلب نمذجة المعادلات الهيكلية الصغرى الجزئية إطار نظري قوي عكس النمذجة القائمة على التباين المشترك (CB-SEM).
- ✓ البرنامج يدعم التعامل مع بيانات قياسية أو شبه قياسية (ترتبية-ترتيبية)، بيانات مقيسة.

➢ أما بالنسبة لسبب اختيارنا للطبعة الرابعة لبرنامج Smart PLS، يعود ذلك إلى أفضلية التحسينات الطارئ عليه، أولها تصليح مشكل المحاذاة والترجمة الجيدة حين الانتقال إلى اللغة العربية مقارنة بالطبعة الثالثة للبرنامج، إضافة إلى سلاسة وسهولته.

المطلب الثاني: تصميم الاستبانة وترميز الفقرات

تم تجزئة الاستبانة الخاصة بدراستنا إلى أربعة أجزاء، حيث قمنا بترميز فقراتها حتى يسهل علينا تحليل النتائج كما هو موضح أدناه:

- **تصميم الاستبانة:** صممت وأعدت لغرض الدراسة فشملت (46) عبارة مقسمة على أربعة أجزاء:

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 (01-06).

[1] Sarstedt Marko, Hair Joe, **Christian Ringle, Partial Least Structural Equation** Modeling, Sage Publications Inc, 2nd Editio, Thousand Oaks, 2017, p 11.

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

-سرية البيانات الفقرات (7-11)، -التوافر والديمومة الفقرات (12-16)،
-تتبع الأثر الفقرات (17-21)، -التكنولوجيا المستخدمة الفقرات (22-26)،
-احترام الخصوصية الفقرات (27-31)،

3-الجزء الثالث: احتوى **المتغير الوسيطي (ثقة العملاء)**: الفقرات (32-41).

4-الجزء الرابع: **شمل المتغير التابع (الخدمات الإلكترونية المصرفية)**: الفقرات (42-46).

2-1 ترميز الفقرات للمتغير المستقل: "الأمن السيبراني"

الفقرات أو المؤشرات حسب تسميتها في برنامج Spss v26

الجدول رقم (III-3): ترميز فقرات أو مؤشرات أبعاد المتغير المستقل الأمن السيبراني

الرمز	المعنى	الفقرات
CON	سرية البيانات	CON1- CON2- CON3- CON4- CON5
AVA	التوافر والديمومة	AVA1- AVA2- AVA 3- AVA4- AVA5
TECH	التكنولوجيا المستخدمة	TECH1- TECH2- TECH3- TECH4- TECH5
PRI	احترام الخصوصية	PRI1- PRI2- PRI3- PRI4- PRI5
TRA	تتبع الأثر	TRA1- TRA2- TRA3- TRA4- TRA5

المصدر: من اعداد الطالب بالاعتماد على مخرجات برنامج Spss v26.

3-1 ترميز الفقرات للمتغير الوسيطي "ثقة العملاء"

الفقرات أو المؤشرات حسب تسميتها في برنامج Spss v26

الجدول رقم (III-4): ترميز فقرات أو مؤشرات المتغير الوسيطي: " ثقة العملاء"

الرمز	المعنى	الفقرات
CNFC	البعد المعرفي للثقة	CNFC1- CNFC2- CNFC3- CNFC4- CNFC5
CNFE	البعد العاطفي للثقة	CNFE1- CNFE2- CNFE3- CNFE4- CNFE5

المصدر: من اعداد الطالب اعتمادا على مخرجات برنامج Spss v26

4-1 ترميز الفقرات الكامنة والمقاسة للمتغير التابع: "الخدمات الإلكترونية المصرفية"

الفقرات أو المؤشرات حسب تسميتها في برنامج Spss v26

الجدول رقم (III–5): ترميز فقرات أو مؤشرات الخدمات الإلكترونية المصرفية.

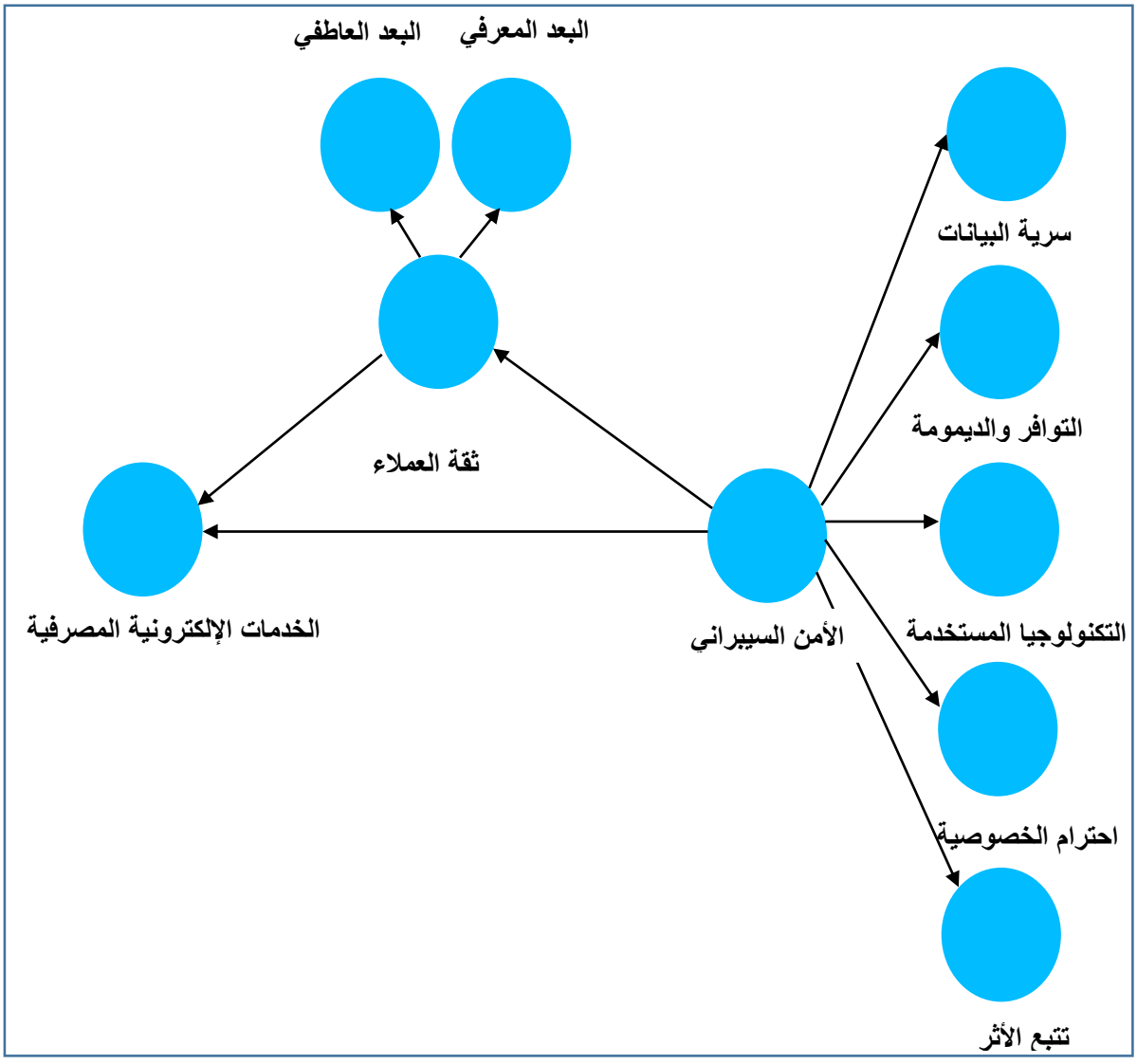
الرمز	المعنى	الفقرات
EBS	الخدمات الإلكترونية المصرفية	EBS1- EBS2- EBS3- EBS4- EBS5

المصدر: من اعداد الطالب اعتمادا على مخرجات برنامج Spss v26

المطلب الثالث: النموذج المقترح للدراسة

بالاعتماد على مخرجات برنامج Smart PLS.4، الشكل البياني يوضح النموذج المقترح للدراسة والذي يتكون من: متغيرات الدراسة (الأمن السيبراني)، (الثقة)، (الخدمات الإلكترونية المصرفية)، كالآتي:

الشكل رقم (III–12): النموذج المقترح للدراسة.



المصدر: من اعداد الطالب بالاعتماد على مخرجات برنامج Smart PLS.4

المبحث الثالث: اختبار أداة الدراسة والنموذج النظري العام المقترح للدراسة

في هذه المرحلة سيتم اختبار أداة الدراسة ومدى صدقها وثباتها، مستخدمين بذلك مقياس ليكارت الخماسي مع اختبار النموذج النظري العام المقترح للدراسة كما يلي:

المطلب الأول: سلم القياس العبارات مع صدق وثبات أداة الاستبانة

أولا: سلم القياس العبارات

استخدمت الدراسة مقياس ليكارت Lekartscale الخماسي فقد أُعطيت الدرجات التالية للفقرات المستخدمة في الاستبانة:

درجة (5)	درجة (4)	درجة (3)	درجة (2)	درجة (1)
موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة

الدرجات هي من (1 إلى 5) كما يلي:

-درجة (1) للإجابة: غير موافق بشدة.

-درجة (2) للإجابة: غير موافق.

-درجة (3) للإجابة: محايد.

-درجة (4) للإجابة: موافق.

-درجة (5) للإجابة: موافق بشدة.

وحددت رتب ودرجات لهذه المتوسطات حسب المعيار التالي:

تم تقسيم مدى الاستجابة (1-5) إلى ثلاثة فئات متساوية الطول، بناء على القاعدة الحسابية التالية:

طول الفئة = المدى / عدد الفئات. وبذلك يكون طول الفئة = 3/4=1.33 وبالتالي يكون مقياس التحليل كالتالي:

- أعتبر المتوسط الحسابي ذو درجة **منخفضة** إذا تراوح بين: [1,00 – 2,33]
- أعتبر المتوسط الحسابي ذو درجة **متوسطة** إذا تراوح بين: [2,34 – 3,66]
- أعتبر المتوسط الحسابي ذو درجة **مرتفعة** إذا تراوح بين: [3,67 – 5,00]

ثانيا: صدق وثبات أداة الاستبانة

2-1 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 ومعسكر جامعة الأغواط وجامعة دهوك بدولة العراق ومن ذوي الاختصاص والخبرة الميدانية كما هو موضح في (الملحق رقم:3 و4)، 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 مؤشرا على الصدق الظاهري للأداة.

وعليه، نتائج تحكيم الاستبيان للمحكمين الخمسة كما هي موضحة في الجدول التالي رقم (III-6):

الجدول رقم (III-6): صدق الاستبيان لمتغيرات الدراسة حسب المحكمين

الأبعاد		رقم العبارة	تقيس	لا تقيس	صدق العبارة
الأمن السيبراني	سرية البيانات	01	05	00	1
		02	05	00	1
		03	04	01	0.88
		04	05	00	1
		05	05	00	1
	التوافر والديمومة	01	05	00	1
		02	04	01	0.88
		03	03	02	0.66
		04	03	02	0.66
		05	05	00	1
	التكنولوجيا المستخدمة	01	05	00	1
		02	04	01	0.88
		03	05	00	1
		03	03	02	0.66
		05	05	00	1
		01	05	00	1

	احترام الخصوصية	02	05	00	1
		03	03	02	0.66
		04	05	00	1
		05	04	01	0.88
	تتبع الأثر	01	05	00	1
		02	05	00	1
		03	04	01	0.88
		04	05	00	1
		05	04	01	0.88
ثقة العملاء	البعد المعرفي	01	05	00	1
		02	04	01	0.88
		03	05	00	1
		04	05	00	1
		05	04	01	0.88
	البعد العاطفي	01	05	00	1
		02	04	01	0.88
		03	03	02	0.66
		04	03	02	0.66
		05	05	00	1
الخدمات الإلكترونية المصرفية		01	05	00	1
		02	05	00	1
		03	03	02	0.66
		04	04	01	0.88
		05	05	00	1

المصدر: من اعداد الطالب

تتراوح قيمة الصدق بين 0 و1، وتمثل المعاملات التي تفوق نتيجة مقبولة، وبالعودة إلى الجدول رقم: (14) يمكن ملاحظة أن عبارات بعد سرية البيانات نالت نسبة قبول 97%، بعد التوافر والديمومة 84%، تتبع الأثر 95%، التكنولوجيا المستخدمة 90%، احترام الخصوصية 90%، يعني بنسبة قبول عام لعبارات أبعاد الأمن

السيبراني بنسبة 91%، أما بالنسبة للبعد المعرفي للثقة قابلته نسبة 95%، البعد العاطفي للثقة نسبة 84%، الخدمات الإلكترونية المصرفية نسبة 90%، ما يدل الجدول على أن المستوى الكلي للاستبيان يشير إلى 90%، وهي نسبة قبول عالية تؤكد أن هذا الاستبيان قد حظي بقبول كبير لدى الأساتذة المحكمين، وأن الآراء كانت مشجعة وتصب في اتجاه اعتماده في جمع البيانات.

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]، وفي تعريف آخر يقصد بالثبات أن قياس الظاهرة من خلال الاستبيان يعطي نتائج مستقرة ومتشابهة كل مرة، بتعبير آخر اتساق في نتائج الاستبيان، فلا يمكن الاعتماد على المقياس إلا إذا تم تكرار تطبيق الاختبار بنفس الشروط وتم الحصول على نتائج نفسها، لذلك يعد اختبار الثبات خطوة مهمة لأنه يشير إلى الموثوقية والاتساق عبر أجزاء الاستبيان،[2] ويعد معامل ألفا كورنباخ كمقياس للاتساق الداخلي الأكثر شيوعا وأنسب مقياس عند استخدام موازين ليكارت، كما تتراوح قيمة المعامل بين (0) التي تعني أن الاستبيان غير ثابت تماما و(1) تعني أن الثبات تام للاستبيان، كما يقترح الكثيرين من الإحصائيين أن ثبات الاستبيان يحتاج إلى بلوغ معامل ألفاكرونباخ قيمة أو تفوق 0.70 ضمن مجال الموثوقية العالية.[3]

وبهدف التأكد من ثبات أداة الاستبيان المعدة للقياس، تم إجراء اختبار الاتساق الداخلي لعبارات الاستبيان وفق معامل ألفاكرونباخ، وعلى ضوء ذلك تحصلنا على القيم المذكورة في الجدولين التاليين.

*** اختبار ألفاكروميخ:**

للتأكد من ثبات أداة القياس المستخدمة في الدراسة تم احتساب معامل (ألفاكرونباخ) لأبعاد الدراسة باستثناء المعلومات والبيانات العامة، إذ أظهرت نتائج التحليل الإحصائي أن مستوى الثبات كان عاليا وفقا للمعايير الإحصائية المتعارف عليها حيث بلغ 855, وهو ما يفوق 85% مما يجعل المعيار مقبول جدا.

الجدول رقم (III-7): اختبار ألفاكروميخ الكلي للفقرات

Statistiques de fiabilité

Alpha de Cronbach's	Nombre d'éléments
,855	40

المصدر: من اعداد الطالب بناء على مخرجات برنامج Spss v26

[1]Ahmad Shammont, **Evaluating an Extended relationship Marketing Model for Arab Guests of Five star hotels**, PHD Thesis, school of Hospital ,Tourism and Marketing, Victoria University-Melbourne, 2007, p 146.

[2] Hamed Taherdoost**, Validity and Reliability of the Research Instrument, How to Test the Validation of a How to Test the Validation of a**, International Journal of Academic Research in Management, Vol 5, N 3, 2016, p 23.

[3] Perry Hilton, Isabella Murray, Charlotte Brownlow**, SPSS Explained**, 2nd Edition, London, 2014, p 352.

حيث كانت ثبات الفقرات كما هو موضح في الجدول التالي رقم (III-8) كما يلي:

الجدول رقم (III-8): معاملات ألفا كرومباخ التفصيلية لأبعاد ومحاور الدراسة

المحور	عدد الفقرات	معامل الثبات ألفا كرومباخ
المحور الأول: الأمن السيبراني في عناصره:	25 فقرة موزعة كالتالي:	
- سرية البيانات	05 فقرات	0.907
- التوافر والديمومة	05 فقرات	0.805
- التكنولوجيا المستخدمة	05 فقرتين	0.806
- احترام الخصوصية	05 فقرات	0.810
- تتبع الأثر	05 فقرات	0.806
المحور الثاني: ثقة العملاء ببعديها:	10 فقرات موزعة كالتالي:	
- البعد المعرفي	05 فقرات	0.786
- البعد العاطفي	05 فقرات	0.796
المحور الثالث: الخدمات الإلكترونية المصرفية	05 فقرات	0.799

المصدر: من اعداد الطالب بناء على مخرجات برنامج SPSS V26

من خلال الجدولين السابقين رقم: (III-7 وIII-8)، تبين لنا أن معاملات الثبات ألفا كرونباخ قد تجاوزت 0.70 في كل المحاور، ما يعني أن الثبات مقبول لاستبيان الدراسة.

المطلب الثاني: اختبارات نموذج القياس للدراسة

تمر عملية التحليل باستخدام برنامج التحليل الاحصائي (Smart PLS.4) بمرحليتين أوليتين: المرحلة الأولى تستهل باختبار نموذج القياس، ثم في المرحلة الثانية تقييم النموذج الهيكلي، وعلى هذا الأساس يخصص هذا المطلب لاختبار صدق وثبات نموذج القياس.

1. تعريف النموذج القياسي (Measurement Model)

يمثل نموذج القياس وفق أسلوب النمذجة بالمعادلات الهيكلية الجزء الخارجي الذي يرتبط ارتباطا وثيقا بالنموذج الهيكلي، حيث يعتبر نموذج القياس أداة رئيسية تهتم بمعالجة وتحديد العلاقة بين متغيرات الدراسة الكامنة مع المتغيرات المشاهدة، بمعنى آخر يضطلع نموذج القياس بتحديد العلاقات بين المتغيرات الكامنة التي تعني متغيرات الدراسة الرئيسية المستقلة أو التابعة مع مؤشرات قياسها أو الدلالة عليها والتي تسمى المتغيرات المشاهدة (عبارات الأسئلة في الاستبيان).

2. اختبار النموذج القياسي:

باستخدام البرنامج الاحصائي (Smart PLS.4) فان تحليل البيانات يمر عبر مرحلتين لتأكيد جودة نموذج القياس للدراسة ومدى موثوقيته في تفسير العلاقات المفترضة بين متغيرات الدراسة، وبعد اختبار موثوقية وصدق نموذج القياس أول خطوة في مسار المعالجة الإحصائية، حيث يرتكز إجراء تقييم مدى موثوقية وصدق نموذج القياس على الاختبارات التالية:

-الصدق التقاربي (Convergent Validity).

-الصدق التمايزي (Discriminant Validity).

3. اختبار الصدق التقاربي:

يشير الصدق التقاربي إلى درجة الاتساق والتقارب بين العناصر المشكلة للاستبيان كالأسئلة والمحاور فيما بينها وذلك لقياس المتغيرات أو الدلالة عليها، ويمكن فحص الصدق التقاربي لنموذج القياس من خلال ثلاثة معايير هي:

-معامل التشبع (Factor Loading).

-الموثوقية المركبة (Composite Reliability) (CR).

-متوسط التباين المستخرج (المفسر) (Average Variance Extracted) (AVE).

من خلال الجدول رقم: (17) يمكن تبيان ملخص لقواعد تحقيق الصدق التقاربي كما يلي:

جدول رقم (III-9): ملخص قواعد تحقيق الصدق التقاربي

المعايير	المقياس والعتبة
مؤشر التشبع الانعكاسي معامل التشبع Factor Loading	ينبغي أن يساوي أو يفوق 0.7
موثوقية الاتساق الداخلي أو معامل الثبات المركب Composite Reliability (CR)+ Cronbach's alpha	يكون بمثابة تمثيل جيد لموثوقية تجاوز الحد الأدنى 0.7
الصدق التقاربي متوسط التباين المستخرج (المفسر) (AVE) (Average Variance Extracted).	الحد الأدنى المطلوب لمتوسط التباين المستخرج هو 0.5

Source: Hair joseph, Partial Least Squares Structual Equation Modeling PLS-SEM Using R 1ed, Switzerland: Springer Cham, 2021, P 80.

4. معامل التشبع Factor Loading:

في البداية يتم فحص الاتساق الداخلي لنموذج القياس الخاص بالدراسة من خلال اختبار تشبعات الأسئلة المتعلقة بعبارات المتغيرات، حيث يتعين النظر في مدى تحقيق معاملات التشبع الحد الأدنى المطلوب المقدر بقيمة تساوي أو تفوق 0.70

فيما يلي مخرجات البرنامج الاحصائي (Smart PLS.4) حول معامل التشبع لجميع عبارات نموذج القياس.

فيما يلي نتائج تشبعات العبارات لمتغيرات الدراسة:

جدول رقم (III–10): نتائج تشبعات العبارات لمتغيرات الدراسة

عبارات الأسئلة	معاملات التشبع (Factor Loading) لنموذج الدراسة							
CON1<--- CONI	0.97	0.00	0.00	0.00	0.00	0.00	0.00	0.00
CON2<--- CONI	0.84	0.00	0.00	0.00	0.00	0.00	0.00	0.00
CON3<--- CONI	0.82	0.00	0.00	0.00	0.00	0.00	0.00	0.00
CON4<--- CONI	0.91	0.00	0.00	0.00	0.00	0.00	0.00	0.00
CON5<--- CONI	0.86	0.00	0.00	0.00	0.00	0.00	0.00	0.00
AVA1 <---AVAI	0.00	0.89	0.00	0.00	0.00	0.00	0.00	0.00
AVA2 <---AVAI	0.00	0.52	0.00	0.00	0.00	0.00	0.00	0.00
AVA3<--- AVAI	0.00	0.83	0.00	0.00	0.00	0.00	0.00	0.00
AVA4 <---AVAI	0.00	0.87	0.00	0.00	0.00	0.00	0.00	0.00
AVA5 <---AVAI	0.00	0.88	0.00	0.00	0.00	0.00	0.00	0.00
TECH1<--- TECHI	0.00	0.00	0.75	0.00	0.00	0.00	0.00	0.00
TECH2<--- TECHI	0.00	0.00	0.98	0.00	0.00	0.00	0.00	0.00
TECH3<--- TECHI	0.00	0.00	0.70	0.00	0.00	0.00	0.00	0.00
TECH4<--- TECHI	0.00	0.00	0.94	0.00	0.00	0.00	0.00	0.00
TECH5<--- TECHI	0.00	0.00	0.93	0.00	0.00	0.00	0.00	0.00
PRI1<---PRII	0.00	0.00	0.00	0.71	0.00	0.00	0.00	0.00
PRI2<--- PRII	0.00	0.00	0.00	0.86	0.00	0.00	0.00	0.00
PRI3<--- PRII	0.00	0.00	0.00	0.90	0.00	0.00	0.00	0.00
PRI4<--- PRII	0.00	0.00	0.00	0.91	0.00	0.00	0.00	0.00
PRI5<--- PRII	0.00	0.00	0.00	0.79	0.00	0.00	0.00	0.00
TRA1<--- TRAI	0.00	0.00	0.00	0.93	0.00	0.00	0.00	0.00
TRA2<--- TRAI	0.00	0.00	0.00	0.81	0.00	0.00	0.00	0.00
TRA3<--- TRAI	0.00	0.00	0.00	0.89	0.00	0.00	0.00	0.00
TRA4<--- TRAI	0.00	0.00	0.00	0.87	0.00	0.00	0.00	0.00

0.00	0.00	0.00	0.85	0.00	0.00	0.00	0.00	TRA5<--- TRAI
0.00	0.00	0.87	0.00	0.00	0.00	0.00	0.00	CNFC1<---CNFCI
0.00	0.00	0.56	0.00	0.00	0.00	0.00	0.00	CNFC2<---CNFCI
0.00	0.00	0.80	0.00	0.00	0.00	0.00	0.00	CNFC3<---CNFCI
0.00	0.00	0.84	0.00	0.00	0.00	0.00	0.00	CNFC4<---CNFCI
0.00	0.00	0.85	0.00	0.00	0.00	0.00	0.00	CNFC5<---CNFCI
0.00	0.86	0.00	0.00	0.00	0.00	0.00	0.00	CNFE1<---CNFCI
0.00	0.82	0.00	0.00	0.00	0.00	0.00	0.00	CNFE2<---CNFCI
0.00	0.71	0.00	0.00	0.00	0.00	0.00	0.00	CNFE3<---CNFCI
0.00	0.84	0.00	0.00	0.00	0.00	0.00	0.00	CNFE4<---CNFCI
0.00	0.88	0.00	0.00	0.00	0.00	0.00	0.00	CNFE5<---CNFCI
0.88	0.00	0.00	0.00	0.00	0.00	0.00	0.00	EBS1<---EBSI
0.86	0.00	0.00	0.00	0.00	0.00	0.00	0.00	EBS2<---EBSI
0.88	0.00	0.00	0.00	0.00	0.00	0.00	0.00	EBS3<---EBSI
0.70	0.00	0.00	0.00	0.00	0.00	0.00	0.00	EBS4<---EBSI
0.86	0.00	0.00	0.00	0.00	0.00	0.00	0.00	EBS5<---EBSI

المصدر: من اعداد الطالب بناء على مخرجات برنامج Smart PLS.4

تشير المخرجات الواردة في الجدول رقم: (III-10) إلى أن جميع معاملات التشبع (Factor Loading) الخاصة بعبارات سرية البيانات، تتبع الأثر، التكنولوجيا المستخدمة، احترام الخصوصية، لمتغير الأمن السيبراني، وعبارات البعد العاطفي للثقة لمتغير ثقة العملاء، وعبارات متغير الخدمات الإلكترونية المصرفية، كلها كانت مقبولة وذات دلالة لكونها تفوق الحد الأدنى المحدد بـ: 0.7 باستثناء عبارات AVA2 لمتغير التوافر والديمومة وCNFC2 لمتغير الثقة المعرفية التي لم تبلغ معاملات التشبع الخاصة بهما الحد الأدنى المطلوب 0.7 وعليه يتم حذف العبارتين من نموذج الدراسة.

جدول رقم (III-11): نتائج تشبعات العبارات بعد حذف العبارتين AVA2 وCNFC2

معاملات التشبع (Factor Loading) لنموذج الدراسة								عبارات الأسئلة
0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.98	CON1<--- CONI
0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.83	CON2<--- CONI
0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.82	CON3<--- CONI
0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.90	CON4<--- CONI
0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.87	CON5<--- CONI
0.00	0.00	0.00	0.00	0.00	0.00	0.91	0.00	AVA1 <---AVAI
0.00	0.00	0.00	0.00	0.00	0.00	0.84	0.00	AVA3<--- AVAI
0.00	0.00	0.00	0.00	0.00	0.00	0.87	0.00	AVA4 <---AVAI
0.00	0.00	0.00	0.00	0.00	0.00	0.89	0.00	AVA5 <---AVAI
0.00	0.00	0.00	0.00	0.00	0.76	0.00	0.00	TECH1<--- TECHI

0.00	0.00	0.00	0.00	0.00	0.98	0.00	0.00	TECH2<--- TECHI
0.00	0.00	0.00	0.00	0.00	0.71	0.00	0.00	TECH3<--- TECHI
0.00	0.00	0.00	0.00	0.00	0.93	0.00	0.00	TECH4<--- TECHI
0.00	0.00	0.00	0.00	0.00	0.94	0.00	0.00	TECH5<--- TECHI
0.00	0.00	0.00	0.00	0.70	0.00	0.00	0.00	PRI1<---PRII
0.00	0.00	0.00	0.00	0.86	0.00	0.00	0.00	PRI2<--- PRII
0.00	0.00	0.00	0.00	0.90	0.00	0.00	0.00	PRI3<--- PRII
0.00	0.00	0.00	0.00	0.91	0.00	0.00	0.00	PRI4<--- PRII
0.00	0.00	0.00	0.00	0.80	0.00	0.00	0.00	PRI5<--- PRII
0.00	0.00	0.00	0.94	0.00	0.00	0.00	0.00	TRA1<--- TRAI
0.00	0.00	0.00	0.81	0.00	0.00	0.00	0.00	TRA2<--- TRAI
0.00	0.00	0.00	0.89	0.00	0.00	0.00	0.00	TRA3<--- TRAI
0.00	0.00	0.00	0.88	0.00	0.00	0.00	0.00	TRA4<--- TRAI
0.00	0.00	0.00	0.85	0.00	0.00	0.00	0.00	TRA5<--- TRAI
0.00	0.00	0.89	0.00	0.00	0.00	0.00	0.00	CNFC1<---CNFCI
0.00	0.00	0.81	0.00	0.00	0.00	0.00	0.00	CNFC3<---CNFCI
0.00	0.00	0.85	0.00	0.00	0.00	0.00	0.00	CNFC4<---CNFCI
0.00	0.00	0.86	0.00	0.00	0.00	0.00	0.00	CNFC5<---CNFCI
0.00	0.87	0.00	0.00	0.00	0.00	0.00	0.00	CNFE1<---CNFCI
0.00	0.80	0.00	0.00	0.00	0.00	0.00	0.00	CNFE2<---CNFCI
0.00	0.72	0.00	0.00	0.00	0.00	0.00	0.00	CNFE3<---CNFCI
0.00	0.85	0.00	0.00	0.00	0.00	0.00	0.00	CNFE4<---CNFCI
0.00	0.88	0.00	0.00	0.00	0.00	0.00	0.00	CNFE5<---CNFCI
0.88	0.00	0.00	0.00	0.00	0.00	0.00	0.00	EBS1<---EBSI
0.86	0.00	0.00	0.00	0.00	0.00	0.00	0.00	EBS2<---EBSI
0.88	0.00	0.00	0.00	0.00	0.00	0.00	0.00	EBS3<---EBSI
0.70	0.00	0.00	0.00	0.00	0.00	0.00	0.00	EBS4<---EBSI
0.86	0.00	0.00	0.00	0.00	0.00	0.00	0.00	EBS5<---EBSI

المصدر: من اعداد الطالب بناء على مخرجات برنامج Smart PLS.4

يتضح بناء على النتائج الواردة في الجدول رقم: (III-11) زيادة في معاملات التشبع لعبارات متغير الأمن السيبراني ومتغير ثقة العملاء بعد حذف العبارتين AVA2 وCNFC2 اللتان لم تحققا الحد الأدنى المطلوب.

5. الموثوقية المركبة (CR) Composite Reliability:

يقاس ثبات المقياس من خلال معيار الموثوقية المركبة حيث تشير القيم المرتفعة إلى درجة عالية من الثبات ويشترط أن تتجاوز قيمة هذا المعامل عتبة 0.7

جدول رقم (III–12): نتائج الموثوقية المركبة(CR) لمتغيرات الدراسة

المتغيرات	الأبعاد	ألفا كرونباخ Cronbach's	الموثوقية المركبة (CR) Composite Reliability
الأمن السيبراني	سرية البيانات	0.907	0.93
	التوافر والديمومة	0.810	0.88
	التكنولوجيا المستخدمة	0.806	0.86
	احترام الخصوصية	0.806	0.86
	تتبع الأثر	0.805	0.84
ثقة العملاء	البعد المعرفي	0.786	0.78
	البعد العاطفي	0.796	0.81
الخدمات الإلكترونية المصرفية	الخدمات الإلكترونية المصرفية	0.799	0.82

المصدر: من اعداد الطالب بناء على مخرجات برنامج Smart PLS.4

تشير النتائج في الجدول رقم: (III–12) إلى أن قيم الموثوقية المركبة (CR) للمتغيرات الثلاث معنوية ودالة إحصائيا، حيث تجاوزت جميع الأبعاد الحد الأدنى بمعاملات فاقت 0.7، وينطبق الأمر ذاته على معاملات ألفا كرونباخ التي تجاوزت 0.7 في كل الأبعاد التي تقيس المتغيرات، وهذا يفسر ثبات وترابط العبارات والأبعاد في نموذج القياس أو الدلالة على متغيرات الدراسة الكامنة.

6. متوسط التباين المستخرج (AVE) Average Variance Extracted:

يستخدم متوسط التبيان المستخرج (AVE) أو ما يعرف بصلاحية التقارب للدلالة على صدق البناء (Convergent Validity) على مستوى النموذج البنائي، ويتم حساب مجموع التشبعات المربعة مقسومة على عدد العبارات أو مؤشرات القياس، ويشترط أن تكون قيمة متوسط التباين المستخرج (AVE) أكبر من 0.5 ليتحقق شرط المعنوية وصدق البناء، حيث أن قيمة (AVE) التي تتجاوز المتوسط 0.5 تعني أن أكثر من نصف التباين يعود إلى مؤشراته بمعنى آخر هذا المقياس هو مؤشر على مستوى العلاقة التي تربط المؤشرات الكامنة.

جدول رقم (III–13): نتائج متوسط التباين المستخرج (AVE) لمتغيرات الدراسة

المتغيرات	الأبعاد	متوسط التباين المستخرج (AVE)
الأمن السيبراني	سرية البيانات	0.88
	التوافر والديمومة	0.83
	التكنولوجيا المستخدمة	0.87
	احترام الخصوصية	0.86
	تتبع الأثر	0.87
ثقة العملاء	البعد المعرفي	0.85
	البعد العاطفي	0.71
الخدمات الإلكترونية المصرفية	الخدمات الإلكترونية المصرفية	0.83

المصدر: من اعداد الطالب بناء على مخرجات برنامج Smart PLS.4

نلاحظ من خلال الجدول رقم: (III–13) المتضمن مخرجات متوسط التباين المستخرج (AVE) أن كل الأبعاد قد حظيت بقيم مقبولة ذات معنوية أكبر من 0.5 وذلك هي تعكس مستوى جيد من الصلاحية المتقاربة، مما يعني أن المتغيرات الكامنة كفيلة بشرح أكثر من 50% من تباين المؤشرات المشكلة للبناء، وهذا يعني لنا وجود صلاحية متقاربة قادرة على شرح بياين المؤشرات.

7. الصدق التمايزي (Discriminant Validity): يهدف معيار الصدق التمايزي إلى قياس درجة الاختلافات في تركيبة نموذج القياس، تقييم مدى تميز المتغيرات تجريبيا عن بعضها البعض داخل النموذج الهيكلي، بتعبير آخر فحص مدى التميز الذي تتمتع به المتغيرات أو الأبعاد، وعدم التكرار أو التداخل بين العبارات، حيث يفترض الصدق إعداد وضبط مؤشرات لقياس خاصة بكل بعد أو متغير دون غيره، ولهذا الغرض يمكن اختيار الصدق التمايزي من خلال معايير الجذر التربيعي (Fornell-Lacker) أو التباين بين المؤشرات ومعيار نسبة الارتباطات الغير متجانسة (HTMT).[1]

[1] Hamid Mohamed Rashid, Sami Waqas, Sidek Mohamed, **Discriminant Validity Assessment: Use of Fornell Larcker Criterion Versus HTMT Criterion**, Journal of Physics: Conf Serie 890, 2017, p p 1-5.

8. معيار الجذر التربيعي (Fornell-Lacker): يقوم هذا المعيار على مبدأ مقارنة الجذر التربيعي لمتوسط التباين المستخرج (AVE) مع التركيبات الكامنة الأخرى، ويتحقق الصدق بشرط أن تكون قيمة الجذر التربيعي لمتوسط التباين المشترك أكبر من قيمة الارتباطات الكامنة أخرى أسفله في المصفوفة، وهذا يعني أن هذا المتغير يمثل المفهوم الذي أعد من أجله دون سواه، أكثر من باقي المتغيرات.

جدول رقم (III–14): مصفوفة الجذر التربيعي لمتوسط التباين المستخرج (AVE)

	سرية البيانات	التوافر والديمومة	التكنولوجيا المستخدمة	احترام الخصوصية	تتبع الأثر	البعد المعرفي للثقة	البعد العاطفي للثقة	الخدمات الإلكترونية المصرفية
سرية البيانات	**0.900**							
التوافر والديمومة	0.612	**0.883**						
التكنولوجيا المستخدمة	0.790	0.513	**0.882**					
احترام الخصوصية	0.679	0.689	0.552	**0.883**				
تتبع الأثر	0.868	0.799	0.871	0.679	**0.861**			
البعد المعرفي للثقة	0.849	0.768	0.789	0.680	0.795	**0.854**		
البعد العاطفي للثقة	0.670	0.878	0.761	0.890	0.792	0.799	**0.832**	
الخدمات الإلكترونية المصرفية	0.859	0.884	0.749	0.846	0.626	0.517	0.813	**0.843**

المصدر: من اعداد الطالب بناء على مخرجات برنامج Smart PLS.4

يتضح جليا من خلال الجدول رقم: **(III–14)** أن قيمة الجذر التربيعي لمتوسط التباين المستخرج (AVE) لكل بعد من الأبعاد هو أكبر من الارتباطات الكامنة أسفل البعد، وهذا يعكس اختلاف وحجم تميز كل بعد عن باقي الأبعاد الأخرى في قياس المفهوم المنوط به، **وبالتالي تحقيق الصدق التمايزي** حسب هذا المعيار.

9. التحميل المتقاطع (Cross Loading): يفترض هذا المعيار أن صدق التميز يتوقف على قوة ارتباط العنصر على البنية المرتبطة به الخانة التي تتقاطع فيها العبارة مع المتغير الكامن، في حين يضعف هذا التحميل مع التركيبات الأخرى، بمعني أن المؤشر له دلالة حصرية مع المتغير الكامن الخاص به.[1]

جدول رقم (III–15): التحميلات المتقاطعة (Cross Loading)

	سرية البيانات	التوافر والديمومة	التكنولوجيا المستخدمة	احترام الخصوصية	تتبع الأثر	البعد المعرفي للثقة	البعد العاطفي للثقة	الخدمات الإلكترونية المصرفية
CON1	**0.909**	0.718	0.741	0.522	0.421	0.722	0.606	0.759
CON2	**0.824**	0.428	0.876	0.840	0.701	0.440	0.548	0.626
CON3	**0.840**	0.812	0.789	0.875	0.427	0.375	0.415	0.421
CON4	**0.879**	0.873	0.577	0.774	0.449	0.523	0.801	0.877
CON5	**0.798**	0.414	0.587	0.777	0.774	0.423	0.458	0.597
AVA1	0.331	**0.872**	0.862	0.754	0.726	0.891	0.623	0.562
AVA3	0.744	**0.861**	0.700	0.775	0.620	0.582	0.659	0.723
AVA4	0.789	**0.880**	0.727	0.770	0.878	0.385	0.447	0.420
AVA5	0.577	**0.838**	0.811	0.211	0.847	0.414	0.124	0.381
TECH1	0.619	0.385	**0.882**	0.798	0.845	0.888	0.774	0.745
TECH2	0.274	0.514	**0.858**	0.789	0.569	0.386	0.789	0.799
TECH3	0.326	0.887	**0.848**	0.859	0.656	0.315	0.799	0.570
TECH4	0.420	0.301	**0.844**	0.222	0.710	0.374	0.159	0.581
TECH5	0.887	0.527	**0.898**	0.654	0.758	0.547	0.121	0.612
PRI1	0.368	0.349	0.428	**0.861**	0.724	0.563	0.725	0.611
PRI2	0.554	0.322	0.424	**0.802**	0.421	0.371	0.779	0.641
PRI3	0.423	0.340	0.519	**0.811**	0.382	0.457	0.772	0.502
PRI4	0.549	0.475	0.503	**0.850**	0.412	0.385	0.700	0.545
PRI5	0.727	0.682	0.647	**0.880**	0.331	0.214	0.774	0.651
TRA1	0.587	0.326	0.700	0.888	**0.860**	0.489	0.212	0.411
TRA2	0.662	0.523	0.441	0.842	**0.865**	0.747	0.458	0.331

[1] Rasoolimanesh Seyyed, **Discriminant Validity Assessment in PLS-SEM: A Comprehensive Composite-Based Approach**, Data Analysis Perspectives Journal, Vol 3, N 2, 2022, p p 1-8.

0.754	0.011	0.520	**0.856**	0.189	0.274	0.423	0.602	**TRA3**
0.789	0.700	0.420	**0.904**	0.125	0.760	0.771	0.728	**TRA4**
0.538	0.741	0.773	**0.862**	0.789	0.712	0.685	0.771	**TRA5**
0.602	0.777	**0.903**	0.712	0.411	0.548	0.508	0.625	**CNFC1**
0.605	0.789	**0.838**	0.541	0.475	0.525	0.658	0.613	**CNFC3**
0.646	0.775	**0.875**	0.575	0.501	0.511	0.652	0.620	**CNFC4**
04.12	0.771	**0.899**	0.114	0.542	0.448	0.512	0.445	**CNFC5**
0.832	0.489	0.889	0.385	0.546	0.719	0.359	0.468	**CNFE1**
0.888	0.496	0.825	0.416	0.588	0.513	0.526	0.775	**CNFE2**
0.812	0.497	0.789	0.287	0.571	0.341	0.421	0.887	**CNFE3**
0.810	0.197	0.845	0.789	0.479	0.408	0.613	0.725	**CNFE4**
0.850	0.189	0.569	0.345	0.387	0.614	0.325	0.778	**CNFE5**
0.900	0.099	0.412	0.569	0.301	0.651	0.456	0.515	**EBS1**
0.855	0.189	0.386	0.385	0.498	0.312	0.478	0.575	**EBS2**
0.854	0.125	0.314	0.315	0.489	0.524	0.375	0.778	**EBS3**
0.824	0.789	0.376	0.472	0.429	0.452	0647	0.679	**EBS4**
0.877	0.345	0.547	0.647	0.789	0.663	0.657	0.555	**EBS5**

المصدر: من اعداد الطالب بناء على مخرجات برنامج Smart PLS.4

تعقيبا عل مخرجات الجدول رقم: (III-15) يمكن القول أن كل القيم الواردة في الخانات التي تتقاطع فيها العبارات مع الأبعاد الخاصة بالأمن السيبراني وثقة العملاء والخدمات الإلكترونية المصرفية هي قيم أكبر مقارنة مع القيمة التي تسجلها مع مكون آخر، مما يدل على تميز المؤشرات وانفرادها بقايس الأبعاد الخاصة بها حصريا، وهي نتائج تفيد بتحقق الصدق الصدق التمايزي لنموذج القياس حسب هذا المعيار.

10. معيار الارتباطات الغير متجانسة الأحادية (HTMT):

(Heterotrait-heteromethod correlatio/smonotrait-hetromethod correlations HTMT)

هذا المعيار يمثل واحدا من المعايير التي تهتم بقياس الصدق التمايزي بناء على حساب: القيمة المتوسطة لارتباطات المؤشر عبر تركيبات الغير متجانسة (التي تقيس المتغيرات الأخرى) بالنسبة إلى القيمة المتوسطة لارتباطات المؤشرات أحادية الأسلوب (التي تقيس نفس المتغير)، وهذا في سياق حدد معامل لتقييم صدق التمايز بقيمة ينبغي أن تكون أقل من 0.9.[1]

[1] Jorg Henseler, Christian Ringle, Marko Sarstedt, **A New Criterion for Assissing Discriminant Validity in Variance-based Structual Equation Modeling,** Journal if the Academy of Marketing Science, Vol 43, N 1, 2015, P P 115-135.

جدول رقم (III-16): نتائج معيار الارتباطات الغير متجانسة (HTMT)

	سرية البيانات	التوافر والديمومة	احترام الخصوصية	التكنولوجيا المستخدمة	تتبع الأثر	البعد المعرفي للثقة	البعد العاطفي للثقة	الخدمات الإلكترونية المصرفية
سرية البيانات	0.890							
التوافر والديمومة	0.798	0.873						
احترام الخصوصية	0.901	0.835	0.889					
التكنولوجيا المستخدمة	0.682	0.591	0.650	0.883				
تتبع الأثر	0.678	0.599	0.875	0.600	0.861			
البعد المعرفي للثقة	0.753	0.674	0.690	0.678	0.799	0.854		
البعد العاطفي للثقة	0.775	0.790	0.572	0.798	0.794	0.791	0.832	
الخدمات الإلكترونية المصرفية	0.861	0.889	0.651	0.642	0.819	0.510	0.712	0.843

المصدر: من اعداد الطالب بناء على مخرجات برنامج Smart PLS.4

يتبين من خلال الجدول رقم: (III-16) أن كل القيم المسجلة لم تتجاوز الحد الأقصى المنصوص عليه وفق هذا المعيار 0.9 وبهذا فإن نموذج القياس يستوفي شروط الصدق التمايزي.

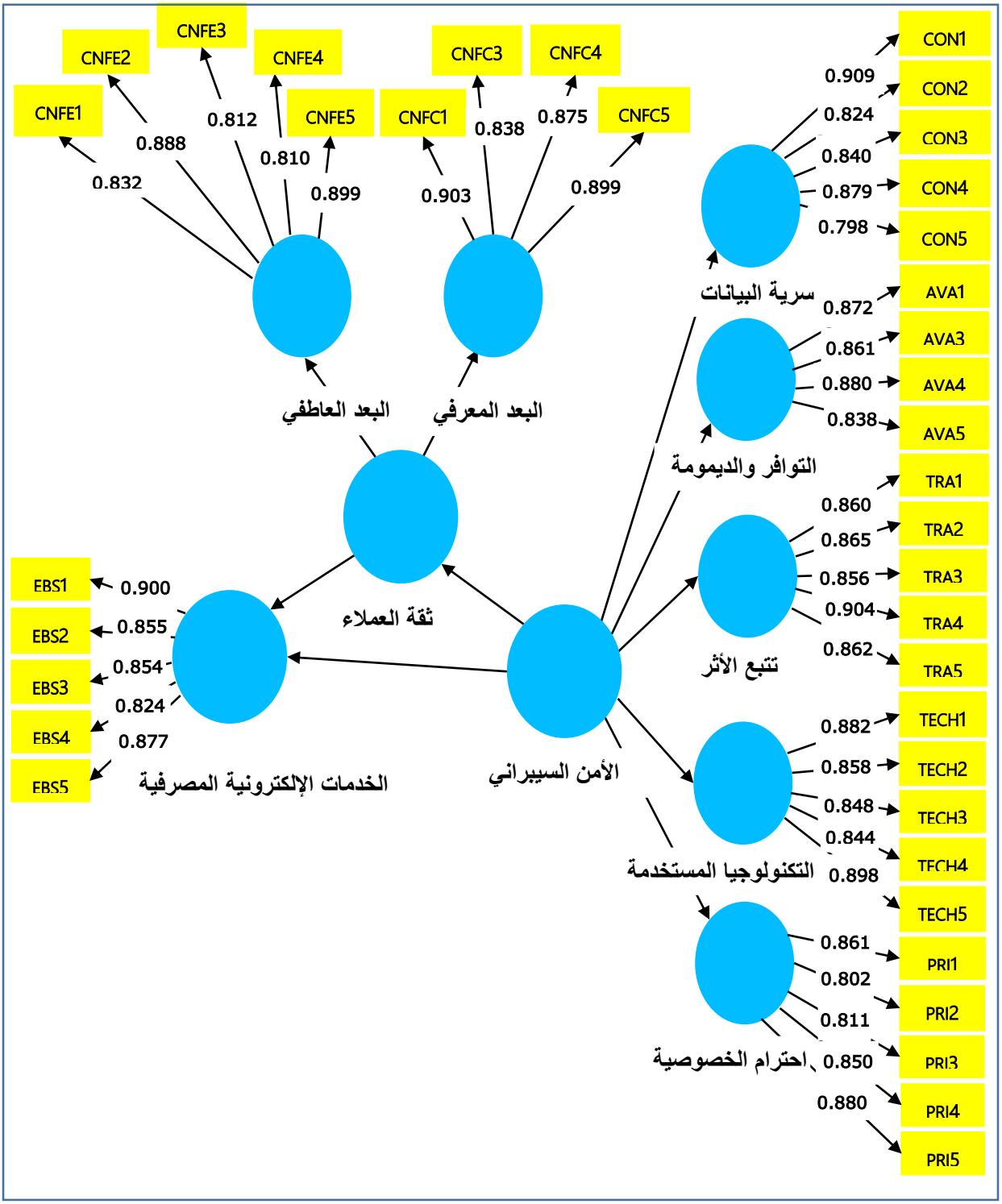
من خلال ما سبق، واستنادا إلى نتائج الاختبارات المتعلقة بالصدق التقاربي والصدق التمايزي لتقييم نموذج القياس الخاص بالدراسة، يمكن التأكيد على جودة نموذج القياس بكل مكوناته، وهذا يفتح الباب على المستوى الاجرائي لبدء مرحلة تحليل النموذج الهيكلي (Structual Model) ضمن المطلوب الموالي:

المطلب الثالث: اختبار النموذج الهيكلي للدراسة

تعقب مرحلة اختبار الصدق لنموذج القياس في الدراسة، الانتقال إلى مرحلة تقييم النموذج الهيكلي للدراسة من خلال مجموعة من المعايير المعتمدة.

1. **تعريف النموذج الهيكلي (Structual Model)**: وهو الجزء الداخلي من النموذج الذي يفسر العلاقات السببية الناشئة بين متغيرات الدراسة الكامنة، بمعنى آخر توضيح طبيعة العلاقة بين المتغيرات المستقلة والتابعة والوسيطية، وكذلك بين نسبة الأثر ومعامل التفسير لكل من المتغيرات المستقلة في المتغيرات التابعة، كما هو موضح في الشكل بعد حذف العبارتين AVA2 وCNFC2 التي لا تلبي معامل التشبع المطلوب.

شكل رقم (III–13): النموذج الهيكلي للدراسة



من اعداد الطالب بناء على مخرجات برنامج Smart PLS.4

2. اختبار النموذج الهيكلي:

عقب النتائج المقبولة في اختبار الصدق التقاربي والتمايزي للنموذج القياسي فإن تقييم جودة النموذج الهيكلي لا يقل أهمية عن تقييم جودة نموذج القياس، وفي هذا الإطار يقوم تقييم النموذج الهيكلي على مبدأ تحري القدرات التنبؤية لنموذج الدراسة والعلاقات بين المتغيرات، بالاعتماد على المعايير الموالية:

1.2. اختبار معامل التحديد R^2:

يعد هذا الاختبار أحد المعايير المهمة التي تبحث في كفاءة النموذج الهيكلي، من خلال فحص درجة تفسير المتغير المستقل للتباينات في المتغير التابع، وتأخذ قيمة معامل التحديد أو التباين مربع قيمة تتراوح بين (1و0) والتي يمكن التعليق عليها بنسبة مؤوية من التأثير في المتغير التابع تفسرها المتغيرات المستقلة داخل النموذج.[1] كما تشير المستويات إلى ما يلي:

R^2 (أقل من 0.25 قيم ضعيفة)

R^2 (من 0.25 إلى 0.50 قيم متوسطة)

R^2 (أكبر من 0.75 قيم جيدة)

جدول رقم (III–17): نتائج معامل التحديد R^2

المتغيرات	R Square
البعد المعرفي للثقة	0.875
البعد العاطفي للثقة	0.649
الخدمات الإلكترونية المصرفية	0.718

المصدر: من اعداد الطالب بناء على مخرجات برنامج Smart PLS.4

نتائج الجدول رقم: (III–17) تشير أن معاملات التحديد الخاصة بثقة العملاء تراوحت بين 0.64 و0.87 وهي معاملات تأثير قوية، تعني أن متغير الأمن السيبراني يفسر 64% من تغير في الثقة العاطفية و87% من التغير في الثقة المعرفية، أما بالنسبة للتغير في ثقة العملاء فيعزى تفسيره إلى متغير الخدمات الإلكترونية المصرفية بمعامل 0.71 تقابله النسبة المؤوية 71%.

2.2. حجم الأثر f^2 (Effet Size):

يفحص هذا المعيار حجم تأثير بنية خارجية محددة على الهيكل الداخلي للنموذج إذا تم حذفه أو إسقاطه من النموذج، ويعتبر آخر تعبر قيمة حجم الأثر f^2 عن مقدار التأثير الذي يخلفه متغير مستقل بعينه على المتغير التابع،

[1] Filho Figueiredo, Silva Junior, Rocha Enivaldo, **What is R2 all about, Leviathan (Sao Paulo)**, N 3, 2011, P P 60-68.

حيث يتم تقييم التأثير حسب نتائج المعاملات المحصل عليها ضمن المجالات التالية:[1]

(0.02–0.15) تأثير ضعيف (صغير).

(0.15–0.35) تأثير متوسط.

(أكثر من 0.35) تأثير قوي (كبير).

جدول رقم (III–18): نتائج حجم الأثر f^2

المتغيرات	قوة التأثير f^2	حجم التأثير
الأمن السيبراني===البعد المعرفي للثقة	0.80	كبير
الأمن السيبراني===البعد العاطفي للثقة	0.75	كبير
الأمن السيبراني===الخدمات الإلكترونية المصرفية	0.86	كبير

المصدر: من اعداد الطالب بناء على مخرجات برنامج Smart PLS.4

حسب النتائج الواردة في الجدول رقم: (III–18) نلاحظ أن حجم الأثر f^2 كبير للمتغير المستقل الأمن السيبراني على كل الأبعاد الأخرى بقيم تجاوزت 0.35 حيث كان التأثر على أبعاد متغير ثقة العملاء (البعد المعرفي للثقة 0.80 والبعد العاطفي للثقة 0.75)، وكان التأثير أيضا كبير على بعد الخدمات الإلكترونية المصرفية بـ: 0.86.

3.2. اختبار التعدد الخطي (The Collinearity):

يهدف هذا الاختيار إلى التأكد من عدم وجود مشكل التعدد الخطي، الذي يعني وجود علاقة خطية وتداخل بين المتغيرات المستقلة الذي يتناقض مع مبدأ عدم التداخل الذي ينشأ عنه نتائج مغلوطة، ومن أجل اكتشاف ذلك يتم الاستعانة بمعامل تضخيم التباين (Vif)، حيث يفترض هذا الاختبار أن تكون القيم أقل من الحد الأقصى المحدد عند العتبة (5).[2]

والجدول التالي رقم (27) يبين نتائج اختبار العلاقة الخطية بطريقة (Vif) كما يلي:

[1] Ken Wong Kay Kwong, **Mediation Analysis, Categorical Moderation Analysis, and Higher Order Constructs Modeling in Partial Least Squares Structural Equation Modeling (PLS-SEM): A B2B Example Using Smart PLS**, Marketing Bulletin, Vol 26, N 1, 2016, P P 1-22.

[2] Amirhosein Mosavi, Assefa Melesse, Subodh Chandra Pal, **Flash Flood Susceptibility Modeling Using New Approaches of Hybrid and Ensemble Tree-Based Machine Learning Algorithms**, Journal Remote Sens, Vol 12, N 3568, 2020, P 3106.

جدول رقم (III–19): نتائج اختبار العلاقة الخطية بطريقة (Vif)

العبارات	Vif
CON1	1.206
CON2	2.101
CON3	1.584
CON4	2.004
CON5	3.012
AVA1	1.716
AVA3	3.124
AVA4	3.119
AVA5	1.899
TECH1	3.212
TECH2	3.100
TECH3	2.998
TECH4	3.987
TECH5	1.201
PRI1	1.111
PRI2	2.514
PRI3	3.360
PRI4	2.119
PRI5	3.900
TRA1	2.248
TRA2	3.556
TRA3	2.126
TRA4	1.877

1.582	TRA5
3.125	CNFC1
2.215	CNFC3
3.335	CNFC4
1.598	CNFC5
3.655	CNFE1
2.265	CNFE2
1.258	CNFE3
1.700	CNFE4
1.010	CNFE5
1.001	EBS1
1.598	EBS2
2.154	EBS3
3.353	EBS4
1.115	EBS5

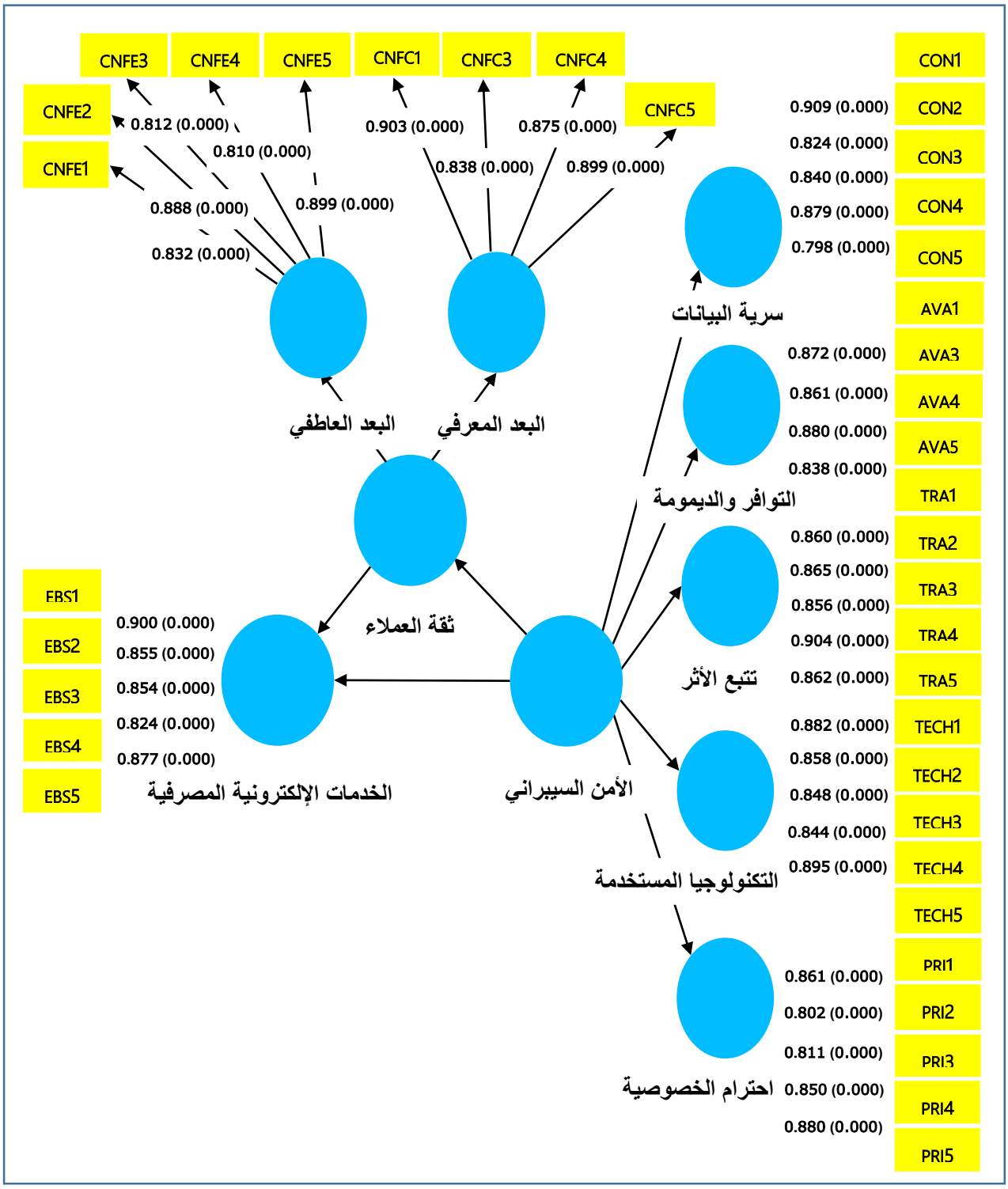
المصدر: من اعداد الطالب بناء على مخرجات برنامج Smart PLS.4

كشفت النتائج الواردة في الجدول رقم: (III-19) أن معاملات التضخم للتباين لكل عبارات الاستبيان أقل من العتبة (5) وهذا يشير إلى خلو نموذج الدراسة من مشكلة التعدد الخطي.

4.2. مسارات النموذج الهيكلي الخارجي:

من بين الاعتبارات المهمة لمسار النمذجة وفق طريقة المربعات الصغرى الجزئية هو تسهيل عملية التنبؤ، لذلك يتم البحث في معاملات المسارات لتحديد قوة وأهمية العلاقات المفترضة بين المتغيرات، حيث تستخدم نتائج تحليل المسار الخارجي للهيكل لتقديم تفسيرات أكثر تفصيلا مثلما هو موضح في الشكل الذي يوضح معاملات المسارات التي تربط بين المتغيرات الكامنة والمتغيرات المشاهدة.

الشكل رقم (III–14): نموذج معاملات المسار المعيارية للنموذج الخارجي



المصدر: من اعداد الطالب بناء على مخرجات برنامج Smart PLS.4

من خلال البرنامج الإحصائي (Smart PLS.4) يمكن إنشاء إحصاءات لاختبار أهمية العلاقات بين المتغيرات الكامنة مع المتغيرات المشاهدة التي تندرج ضمن النموذج الخارجي، فضلا عن العلاقات بين المتغيرات

الكامنة في النموذج الداخلي ويتم هذا باستخدام تقنية (Bootstrapping) البوتسراب القائمة على طريقة أخذ العينات من العينة الأصلية، حيث يقوم البرنامج بتدوير العينة بغرض خلق عدد من العينات الجديدة افتراضية تصل إلى حد 5000 عينة ومن ثم اختبارها من جديد في النموذج واستخدام نتائج جديدة يمكن مقارنتها بالنتائج الأصلية للتأكد من دقة المعطيات أو النتائج.[1]

جدول رقم (III–20): اختبار نتائج التمهيد لمعاملات المسار

P Values	T Statistics (O/STDEV	Standard Deviation (STDEV)	Sample Mean (M)	Original Sample (O)	الإحصاءات / المتغيرات
0.00	65.86	0.01	0.91	0.91	CON1<--- CON
0.00	28.50	0.02	0.89	0.89	الأمن السيبراني---<CON1
0.00	251.02	0.00	0.82	0.82	CON2<--- CON
0.00	50.15	0.01	0.75	0.75	الأمن السيبراني---<CON2
0.00	70.51	0.01	0.84	0.84	CON3<--- CON
0.00	36.60	0.02	0.80	0.80	الأمن السيبراني---<CON3
0.00	92.10	0.01	0.88	0.88	CON4<--- CON
0.00	62.50	0.01	0.77	0.77	الأمن السيبراني---<CON4
0.00	96.18	0.01	0.80	0.80	CON5<--- CON
0.00	40.14	0.03	0.79	0.79	الأمن السيبراني---<CON5
0.00	75.98	0.01	0.87	0.87	AVA1 <---AVA
0.00	35.02	0.01	0.80	0.80	الأمن السيبراني---> AVA1
0.00	67.44	0.01	0.86	0.86	AVA3<--- AVA
0.00	41.01	0.01	0.78	0.78	الأمن السيبراني---<AVA3
0.00	50.32	0.01	0.88	0.88	AVA4 <---AVA
0.00	68.24	0.02	0.83	0.83	الأمن السيبراني---> AVA4
0.00	49.32	0.01	0.84	0.84	AVA5 <---AVA
0.00	54.20	0.01	0.90	0.90	الأمن السيبراني---> AVA5
0.00	47.35	0.01	0.88	0.88	TECH1<--- TECH
0.00	68.37	0.01	0.80	0.80	الأمن السيبراني---<TECH1
0.00	56.94	0.01	0.86	0.86	TECH2<--- TECH
0.00	66.25	0.01	0.74	0.74	الأمن السيبراني---<TECH2
0.00	53.91	0.01	0.85	0.85	TECH3<--- TECH

[1] Ken Wong Kay, **Parti 87.07 al Least Squares Srtuctural Equation Modeling (PLS-SEM) Technique Using Smart PLS**, Marketing Bullet56.86in, Vol 24, N 1, 2013, P P 1-32.

0.00	112.08	0.01	0.81	0.81	TECH3<---الأمن السيبراني
0.00	58.67	0.01	0.84	0.84	TECH4<--- TECH
0.00	123.10	0.01	0.88	0.88	TECH4<---الأمن السيبراني
0.00	57.68	0.01	0.90	0.90	TECH5<--- TECH
0.00	108.48	0.05	0.85	0.85	TECH5<---الأمن السيبراني
0.00	46.82	0.01	0.86	0.86	PRI1<---PRI
0.00	49.28	0.01	0.91	0.91	PRI1<--الأمن السيبراني
0.00	92.75	0.01	0.80	0.80	PRI2<--- PRI
0.00	58.06	0.01	0.83	0.83	PRI2<---الأمن السيبراني
0.00	106.50	0.01	0.81	0.81	PRI3<--- PRI
0.00	59.80	0.01	0.77	0.77	PRI3<---الأمن السيبراني
0.00	99.27	0.03	0.85	0.85	PRI4<--- PRI
0.00	67.64	0.01	0.79	0.79	PRI4<---الأمن السيبراني
0.00	58.09	0.01	0.88	0.88	PRI5<--- PRI
0.00	70.71	0.01	0.84	0.84	PRI5<---الأمن السيبراني
0.00	72.60	0.01	0.86	0.86	TRA1<--- TRA
0.00	54.20	0.01	0.78	0.78	TRA1<---الأمن السيبراني
0.00	71.58	0.02	0.86	0.86	TRA2<--- TRA
0.00	31.38	0.01	0.85	0.85	TRA2<---الأمن السيبراني
0.00	68.87	0.01	0.86	0.86	TRA3<--- TRA
0.00	70.87	0.01	0.89	0.89	TRA3<---الأمن السيبراني
0.00	51.62	0.01	0.90	0.90	TRA4<--- TRA
0.00	66.34	0.01	0.78	0.78	TRA4<---الأمن السيبراني
0.00	56.72	0.01	0.86	0.86	TRA5<--- TRA
0.00	66.31	0.01	0.82	0.82	TRA5<---الأمن السيبراني
0.00	179.22	0.01	0.82	0.82	CNFC4<---ثقة العملاء
0.00	23.25	0.01	0.90	0.90	CNFC5<---CNFC
0.00	27.89	0.01	0.83	0.83	CNFC5<---ثقة العملاء
0.00	108.23	0.01	0.83	0.83	CNFE1<---CNFC
0.00	77.25	0.01	0.89	0.89	CNFE1<---ثقة العملاء
0.00	12.22	0.01	0.89	0.89	CNFE2<---CNFC
0.00	74.36	0.01	0.79	0.79	CNFE2<---ثقة العملاء
0.00	58.22	0.01	0.81	0.81	CNFE3<---CNFC
0.00	54.78	0.01	0.93	0.93	CNFE3<---ثقة العملاء

0.00	66.77	0.01	0.81	0.81	CNFE4<---CNFC
0.00	56.22	0.01	0.70	0.70	ثقة العملاء<---CNFE4
0.00	14.89	0.01	0.85	0.85	CNFE5<---CNFC
0.00	101.23	0.04	0.81	0.81	ثقة العملاء<---CNFE5
0.00	99.35	0.01	0.90	0.90	EBS1<---EBS
0.00	98.53	0.01	0.88	0.88	الخدمات الإلكترونية المصرفية<---EBS1
0.00	18.12	0.01	0.85	0.85	EBS2<---EBS
0.00	79.98	0.01	0.84	0.84	الخدمات الإلكترونية المصرفية<---EBS2
0.00	44.36	0.01	0.85	0.85	EBS3<---EBS
0.00	89.99	0.01	0.80	0.80	الخدمات الإلكترونية المصرفية<---EBS3
0.00	54.33	0.01	0.82	0.82	EBS4<---EBS
0.00	30.78	0.01	0.78	0.78	الخدمات الإلكترونية المصرفية<---EBS4
0.00	98.10	0.01	0.88	0.88	EBS5<---EBS
0.00	16.32	0.02	0.85	0.85	الخدمات الإلكترونية المصرفية<---EBS5

المصدر: من اعداد الطالب بناء على مخرجات برنامج Smart PLS.4

بينت النتائج المحصل عليها بطريقة التدوير الافتراضي أن كل قيم مسارات العلاقات في النموذج الخارجي بين متغير الأمن السيبراني وأبعاده ومتغير ثقة العملاء ببعديه ومتغير الخدمات الإلكترونية المصرفية ومؤشراته، **هي ذات دلالة معنوية** تحت مستوى 0.01 وقيمة T هي أكبر من 1.96 مع كل المسارات.

5.2. مؤشر قوة التنبؤ (Q^2/Predictive Relevance):

يعد هذا المعيار المؤشر على القدرة التنبؤية للنموذج الذي يستند إلى طريقة النمذجة بالمعادلات الهيكلية بطريقة المربعات الصغرى الجزئية، حيث يفترض وجود قدرات تنبؤية للنموذج من خلال المتغيرات الكامنة التابعة، حيث تشير قيم Q^2 الأكبر من الصفر (0) لمتغير كامن تابع إلى أن النموذج يتمتع بقدرة تنبؤية، وإذا كانت (0) فإن النموذج يفقد إلى القدرة على التنبؤ.[1]

جدول رقم (III-21): مؤشرات التنبؤ للنموذج

المتغيرات	SSO	SSE	$Q^2=(1-SSE/SSO)$
البعد المعرفي للثقة	1120	691.35	**0.62**
البعد العاطفي للثقة	1120	678.78	**0.65**
الخدمات الإلكترونية المصرفية	2400	1509.43	**0.59**

المصدر: من اعداد الطالب بناء على مخرجات برنامج Smart PLS.4

[1] Marko Sarstedt, Christian Ringle, Joseph Franklin Hair, **Partial Least Squares Structural Equation Modeling**, Journals Industrial Management Data Systems, Vol 123, N 12, 2021, P 25.

تشير النتائج المدونة في الجدول رقم: (III-21) أن جميع قيم Q^2 التنبؤية الخاصة بالأبعاد المكونة لأبعاد ثقة العملاء ومتغير الخدمات الإلكترونية المصرفية كلها فوق الصفر (0) تراوحت قيمها بين 0.59 و0.65 وهي نتائج تشير إلى قدرة تنبؤ جيدة يتمتع بها النموذج بصفة عامة.

6.2. مؤشرات جودة المطابقة (GoF):

تعتبر النمذجة بطريقة (SEM-PLS) أحد الطرق الإحصائية الحديثة، وكغيرها من النظريات سعى الباحثون لتطوير مقاييس ونماذج من أجل تقييم النماذج باستخدام نمذجة (SEM-PLS) ومن بين هذه المؤشرات المقترحة كإجراء علمي لفحص مصداقية (SEM-PLS) مؤشر (GoF) الذي يمثل أدلة قياس واختبار للنموذج ككل، حيث دأب الكثير من الباحثين الاستعانة به للتقييم والتحقق من صحة نموذج لتقييم النموذج الهيكلي[1]، إذ يقوم هذا الاختبار على مبدأ تقييم مطابقة النموذج حسب قيم مؤشر (GoF)، حيث يفترض أن يكون النموذج ضعيف الجودة بالنسبة للقيم التي تتراوح بين (0.25-0.5) ومتوسط بالنسبة للقيم التي تتراوح بين (0.25-0.36)، ومستوى مطابقة جيدة عندما تكون القيم أكبر من (0.36)[2]

جدول رقم (III-22): مؤشر جودة المطابقة (GoF)

المتغير التابع	الأبعاد	R^2	AVE
ثقة العملاء	البعد المعرفي للثقة	0.875	0.85
	البعد العاطفي للثقة	0.649	0.71
الخدمات الإلكترونية المصرفية	الخدمات الإلكترونية المصرفية	0.718	0.83
المجموع		**0.74**	**0.79**
$GoF=\sqrt{R2\ X(AVE)}$		**$GoF=\sqrt{0.79X0.74}$= 0.76**	

المصدر: من اعداد الطالب بناء على مخرجات برنامج Smart PLS.4

حسب الجدول رقم: (III-22) فإن مؤشر جودة المطابقة يفسر وجود مستوى جيد من الجودة بقيمة 0.76 والتي تفوق عتبة 0.36 (مطابقة جيدة) ومنه يمكن التأكيد على مصداقية النموذج الهيكلي للدراسة.

[1] Jorg Henseler, Sarstedt Marco, **Goodness of fit Indices for Partial Least Squares Path Modeling**, Computational Statistics, Vol 28, N 02, 2013, P P 565-580.

[2] Martin Wetzels, Gaby Schroder Odekerken, Claudia Oppen, **Using PLS Phath Modeling for Assessing Hierarchical Construct Models: Guidelines and Empirical Illustration MIS Quarterly**, Vol 33, N 1, 2009, P P 177-195.

خلاصة الفصل الثالث:

في هذا الفصل تم صياغة منهجية الدراسة، التي تتبع المنهج الوصفي بوصف الظاهرة وصفا كميا وكيفيا بالطريقة الافتراضية الاستنتاجية التي تكشف العلاقة بين أبعادها، مصممين بذلك أداة الاستبانة لجمع البيانات، حيث تم خلال اختيار عينة عشوائية من مستخدمي البطاقات الإلكترونية لعملاء بنك التنمية المحلية غرداية، وعليه بعد تعريف موجز للبنك محل الدراسة والتطرق لأهدافه ومهامه وهيكله التنظيمي، تم التطرق إلى أنواع البطاقات الإلكترونية الموجودة بالبنك ومختلف الخدمات الإلكترونية المصرفية التي يقدمها لعملائه، وفي هذا الاطار تم تزويد القارئ بمعارف حول محاور السياسة الأمنية السيبرانية المنتهجة للبنك محل الدراسة في النقاط التالية:

- مصدر البطاقات والأجهزة المستخدمة إلكترونيا.
- الشبكات الاتصالية، الإنترنت والهاتف النقال.
- البرمجيات وأنظمة المعلومات.
- أنظمة الدفع الإلكترونية.
- التشفير، التوقيع الرقمي، البصمة الرقمية، جدار النار، النسخ الاحتياطي
- أجهزة منع الدخلاء، الموجهات (الراوتر).
- بروتوكولات الحركات المالية الآمنة، بروتوكولات الطبقات الأمنية، تقنية الفتحات الآمنة.

ليتم بعد ذلك توضيح كيفية قياس متغيرات الدراسة ومختلف الأدوات والأساليب الإحصائية المستخدمة فيها، تم توضيح أسلوب وخصائص النمذجة بالمعادلة الهيكلية SEM المنتهجة في الدراسة، مع تبرير أسباب اختيارنا للبرنامج الاحصائي المتقدم Smart PLS.4 بدلا من برنامج AMOS، وبعد التأكد من ثبات وصدق أداة الدراسة، تم عرض واقتراح النموذج النظري الدراسة، وكذا عرض اختبارات نموذج القياس من خلال:

- الصدق التقاربي (Convergent Validity).
- الصدق التمايزي (Discriminant Validity).

في الأخير ومن خلال مؤشر جودة المطابقة (**GoF**)، تم التوصل إلى وجود مستوى جيد من الجودة ومنه يمكن تأكيد مصداقية النموذج الهيكلي للدراسة.

وعليه، سيتم في الفصل الموالي عرض وتفسير نتائج الدراسة باستخدام مجموعة من الأساليب الإحصائية عن طريق برنامج Spss V26 وبرنامج Smart PLS.4.

الفصل الثاني

تحليل وتفسير نتائج الدراسة الميدانية

تمهيد:

يهدف هذ الفصل إلى تحليل البيانات الاحصائية التي جمعها الطالب، وعرض النتائج التي تم التوصل إليها من خلال الدراسة الميدانية، ومن ثم تحليلها وتفسيرها، وصولا إلى جملة من الاقتراحات المتعلقة بموضوع البحث، عليه سنعرض في هذا الفصل ثلاثة مباحث هي على التوالي:

- المبحث الأول: عرض وتحليل نتائج الخصائص العامة المرتبطة بالاستبيان الموجه للعملاء.
- المبحث الثاني: عرض وتحليل نتائج أبعاد الدراسة.
- المبحث الثالث: اختبار الفرضيات ومناقشة نتائج الدراسة.

المبحث الأول: عرض وتحليل نتائج الخصائص العامة المرتبطة بالاستبيان الموجه للعملاء.

سيتم في هذا المبحث عرض نتائج أداة البحث المتمثلة في الاستبانة وتحليلها في المطلب الأول، في حين يخصص المطلب الثاني: لاختبار الفروض واستخلاص النتائج المتوصل إليها ومنه إعطاء توصيات متعلقة بموضوع الدراسة في المباحث الموالية.

للإجابة على أسئلة الدراسة، استخدم الطالب التقسيم الثلاثي لمستويات الأبعاد المذكورة سلفا، سنحاول عرض نتائج الدراسة اعتمادا على ما تم جمعه من بيانات الاستبانة بعد معالجتها إحصائيا ببرنامج الحزم الاحصائية للعلوم الاجتماعية spss v26. **لمعالجة الخصائص العامة:**

المطلب الأول: عرض وتحليل النتائج المتعلقة بالجنس والعمر

أظهرت نتائج الاستبانة المعلومات الديمغرافية الخاصة بجنس وعمر المستجوبين كالتالي:

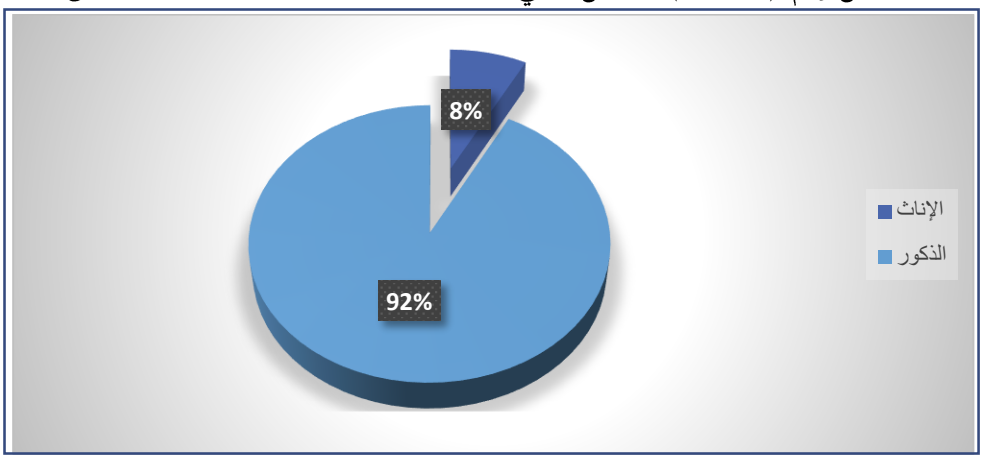
1.1.الجنس:

الجدول رقم (IV-1): تقسيمات عينة البحث حسب الجنس

الجنس	ذكر	أنثى	المجموع
التكرار	180	15	195
النسبة	%92،32	%7،70	%100

المصدر: من اعداد الطالب اعتمادا على معطيات البرنامج spss v26

الشكل رقم (IV-1): تمثيل بياني لتقسيمات عينة البحث حسب الجنس



المصدر: من اعداد الطالب اعتمادا على البرنامج Excel

نلاحظ أن نسبة الإناث 7،70% كانت أقل بكثير من نسبة الذكور 92،32%. يمكن إرجاع سبب النسبة الضعيفة لفئة الإناث في هذه العينة إلى توقيت إجراء الدراسة الميدانية الذي صادف شهر رمضان، أين تقل الحركة نهارا بالنسبة للإناث.

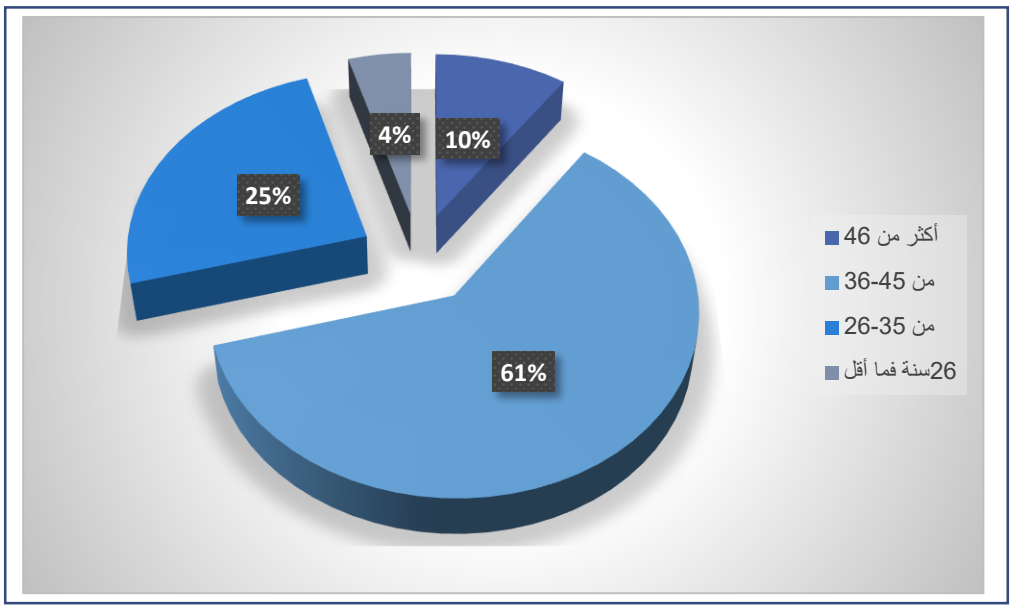
1.2.العمر:

الجدول رقم (IV–2): تقسيمات عينة البحث حسب العمر

الفئـة	أقل من 26	35–26	45–36	أكثر من 46	المجموع
التكرار	9	48	119	19	195
النسبة	%4،61	%24،61	%61،02	%9،74	%100

المصدر: من اعداد الطالب اعتمادا على معطيات البرنامج spss v26

الشكل رقم (IV–2): تمثيل بياني لتقسيمات عينة البحث حسب العمر



المصدر: من اعداد الطالب اعتمادا على البرنامج Excel

الفئة العمرية المستجوبة الغالبة هي فئة ما بين 36–45 سنة بنسبة 61،02%، تليها فئة ما بين 26–45 سنة بنسبة 24،61%، في حين تتوزع النسبة الباقية على الفئة الأقل سنا (أقل من 26 سنة) بنسبة 4،61%. حيث لاحظنا أن الفئة الأقل سنا (أقل من 26 سنة) هي الفئة الأضعف في الإجابة عن الاستبانة، نرجع ذلك إلى عدم استخدامهم للخدمات المصرفية الالكترونية الخاصة بالبنك محل الدراسة، مع العلم أن الأغلبية لهاته الفئة في هذا السن هي عاطلة عن العمل أو هي مقبلة على ذلك، إضافة إلى تواجد عدد منها في مقاعد الدراسة، في حين نلاحظ أن النسبة الأكبر للمجيبين هم من فئة ما بين 36–45 سنة، ويعود ذلك في الغالب لكونهم من الموظفين سواء في القطاع العام أو عاملين بالقطاع الخاص أو أصحاب مهن حرة كالمحاماة والتجارة والحرف والمقاولة وغيرها.

المطلب الثاني: عرض وتحليل النتائج المتعلقة بالمستوى التعليمي والمهنة

أظهرت نتائج الاستبانة المعلومات الديمغرافية الخاصة بالمستوى التعليمي ومهنة المستجوبين كالتالي:

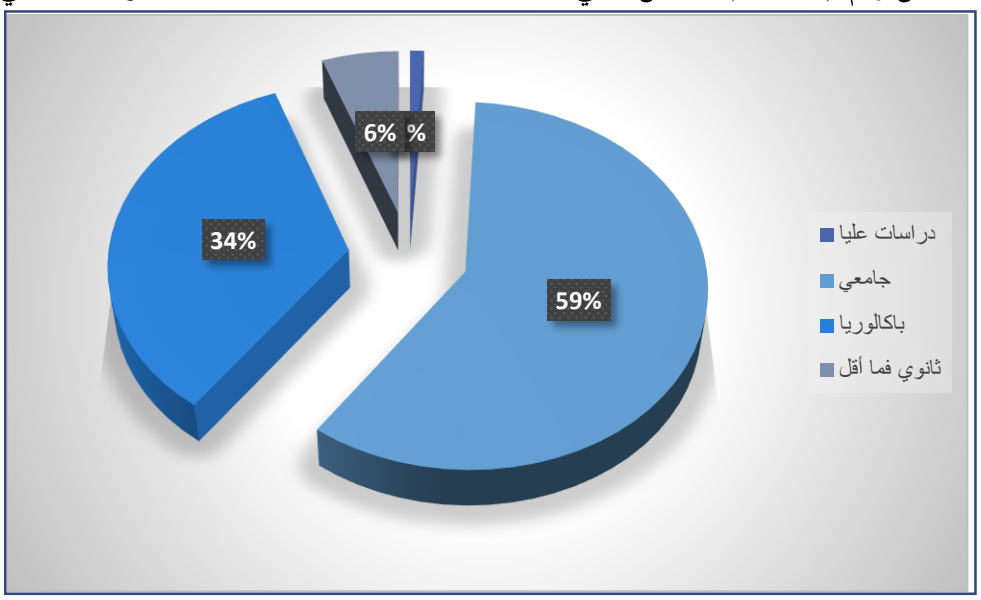
2.1.المستوى التعليمي:

الجدول رقم (IV-3): تقسيمات عينة البحث حسب المستوى التعليمي

المستوى	ثانوي فما أقل	باكالوريا	جامعي	دراسات عليا	المجموع
التكرار	11	67	115	2	195
النسبة	%5،64	%34،35	%58،97	%1،02	%100

المصدر: من اعداد الطالب اعتمادا على معطيات البرنامج spss v26

الشكل رقم (IV-3): تمثيل بياني لتقسيمات عينة البحث حسب المستوى التعليمي



المصدر: من اعداد الطالب اعتمادا على معطيات البرنامج Excel

أعطت نتائج الاستبانة أن النسبة الغالبة من المستجوبين هي من ذوي المستوى الجامعي بنسبة 58،97% والبكالوريا بنسبة 34،357% بينما كانت النسبة ضعيفة لذوي مستوى (ثانوي فما أقل) بنسبة 5،64% وقليلة جدا لذوي مستوى (الدراسات العليا) بنسبة 1،02%، رغم حرص الباحث على توزيع الاستبانة ميدانيا بالبنك محل الدراسة أن تصل إلى مختلف شرائح المجتمع، حيث يرجح الباحث أن الفئة التي لها ثقة في التكنولوجيا وفي التعاملات الإلكترونية هي الفئة العاملة ذات المستوى التعليمي والثقافي (جامعي)، وبالنسبة لقلة نسبة عينة الدراسة لذوي مستوى (الدراسات العليا) 1،01%، يعود ذلك إلى أنه أصلا هاته الفئة قليلة جدا في المجتمع ككل.

2.2.المهنة:

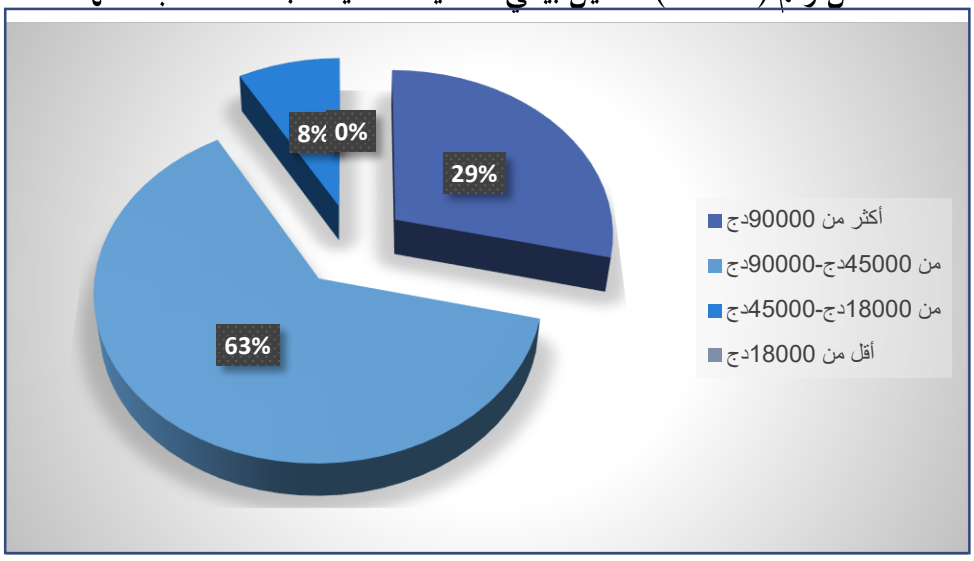
كانت النتائج كما يلي:

الجدول رقم (IV–4): تقسيمات عينة البحث حسب المهنة

المهنة	موظف بالقطاع العام	عامل بالقطاع الخاص	أخرى أذكرها:	تاجر	مقاول	محامي	حرفي	المجموع
التكرار	68	38	89	49	15	16	9	195
النسبة	34،87 %	19،48 %	45.64 %	25،12 %	7,69 %	8,20 %	4,61 %	%100

المصدر: من اعداد الطالب اعتمادا على معطيات البرنامج spss v26

الشكل رقم (IV–4): تمثيل بياني لتقسيمات عينة البحث حسب المهنة



المصدر: من اعداد الطالب اعتمادا على البرنامج Excel

أثبتت نتائج الدراسة أن النسبة الأكبر كانت للعاملين بالمهن الأخرى يعني: (التجار، المحامين، المقاولين، الحرفيين) بنسبة إجمالي 45.64%، تليها نسبة الموظفين بالقطاع العام 34،87%، وفي الأخير نسبة العاملين بالقطاع الخاص 19،48%، يرى الباحث أن ذلك يعود إلى ارتفاع نسبة التجار 25،12% في هاته الفئة بحسب خصوصية المنطقة (غرداية)، كذا امتلاكهم حسابات بنكية وتعاملاتهم المختلفة ببطاقات الدفع والسحب والتحويل الإلكترونية وحيازتهم بالمحلات التجارية على أجهزة نهائي الدفع الإلكتروني (TPE).

المطلب الثالث: عرض وتحليل النتائج المتعلقة بالدخل ومدة التعامل مع البنك

أظهرت نتائج الاستبانة المعلومات الديمغرافية الخاصة بالدخل ومدة تعمل المستجوبين مع البنك كالتالي:

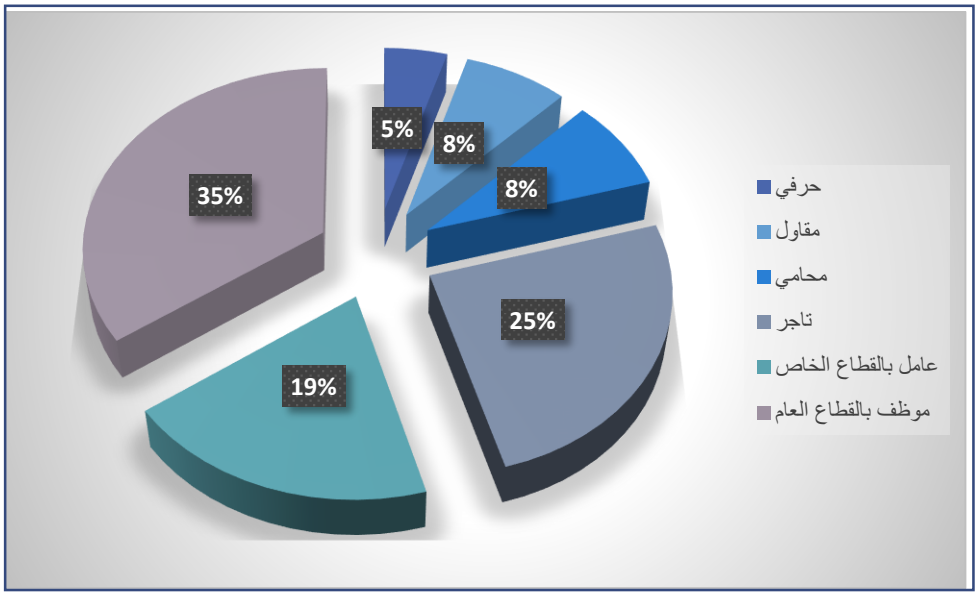
3.1.الدخل:

الجدول رقم (IV-5): تقسيمات عينة البحث حسب الدخل

الدخل	أقل من 18000دج	من 18000دج إلى 45000دج	من 45000دج إلى 90000دج	أكثر من 90000دج	المجموع
التكرار	00	16	123	56	195
النسبة	%0	%8،20	%63،07	%28،71	%100

المصدر: من اعداد الطالب اعتمادا على معطيات البرنامج spss v26

الشكل رقم (IV-5): تمثيل بياني لتقسيمات عينة البحث حسب الدخل



المصدر: من اعداد الطالب اعتمادا على البرنامج Excel

أثبتت نتائج الدراسة أن النسبة الأكبر كانت لذوي الدخل ما بين (45000-90000دج) بنسبة 63،07% تلتها نسبة الدخل الأكثر من 90000دج بنسبة 28،71% ثم تلتها فئة ذوي الدخل ما بين (18000-45000دج) بنسبة 8،20%، بينما انعدمت كليا نسبة ذوي الدخل الأقل من 18000دج، حسب رأي الباحثين أن ارتفاع نسبة الفئة ذات الدخل ما بين (45000دج-90000دج) يرجع إلى كون أغلبهم تجار وكذا موظفي القطاع العام متوسطي الدخل، وأما بالنسبة للانعدام الكلي لنسبة ذوي الدخل الأقل من 18000دج، راجع إلى عزوفهم عن استخدام الخدمات الالكترونية المصرفية نظرا لدخلهم الضعيف.

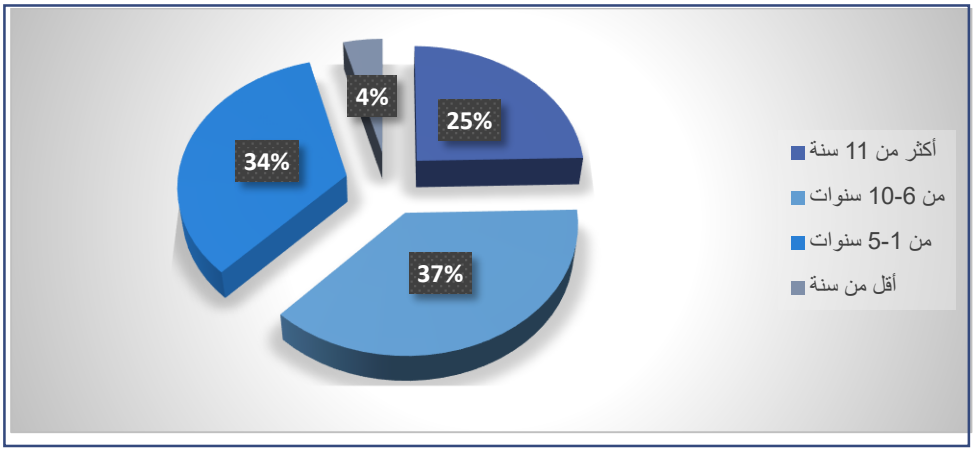
3.2.مدة التعامل مع البنك:

الجدول رقم (IV–6): تقسيمات عينة البحث حسب مدة التعامل مع البنك

الدخل	أقل من سنة	من 1–5 سنوات	من 6–10 سنوات	أكثر من 11 سنة	المجموع
التكرار	8	66	73	48	195
النسبة	%4،10	%33،84	%37،43	%24،61	%100

المصدر: من اعداد الطالب اعتمادا على معطيات البرنامج spss v26

الشكل رقم (IV–6): تمثيل بياني لتقسيمات عينة البحث حسب مدة التعامل مع البنك



المصدر: من اعداد الطالب اعتمادا على البرنامج Excel

من خلال الجدول والشكل السابقين، يتضح أن النسبة الأكبر من المستجوبين من عينة الدراسة كانت للفئة ذات الخبرة في التعامل مع البنك (من 6–10 سنوات) بنسبة 37،43%، تليها فئة (من 1–5 سنوات) بنسبة 33،84%، ثم فئة (الأكثر من 11 سنة) بنسبة 24،61%، وفي الأخير بنسبة ضئيلة لفئة (أقل من سنة) بنسبة 4،10%.

المبحث الثاني: عرض وتحليل نتائج أبعاد الدراسة

في هذا المبحث سنعرض ونحلل نتائج أبعاد متغيرات الدراسة المتحصل عليها كالآتي:

المطلب الأول: عرض وتحليل نتائج أبعاد المتغير المستقل

عرض وتحليل نتائج أبعاد المتغير المستقل "الأمن السيبراني" كانت كما يلي:

1. الإجابة عن السؤال الأول:

- **ما مستويات الاستجابة لأبعاد الأمن السيبراني لدى العملاء؟**

تم استخدام سلم ليكارت الخماسي وحساب المتوسطات الحسابية والانحرافات المعيارية لمعرفية مستويات الاستجابة لأبعاد المفهوم، وقد توصلنا بعد المعالجة الاحصائية إلى ما يلي:

الجدول رقم (IV–7): المتوسطات الحسابية والانحرافات المعيارية لفقرات محور الأمن السيبراني

الرقم	السؤال	المتوسط الحسابي	الانحراف المعياري	الترتيب	الدرجة
7	يحرص البنك على إعطائي رقما سريا خاصا للبطاقة الإلكترونية منذ يوم التسليم.	4,90	,304	1	مرتفعة
8	يتأكد البنك من هويتي وصلاحية دخولي في كل معاملة إلكترونية أقوم بها.	4,24	,655	04	مرتفعة
9	الرقم السري لبطاقتي الإلكترونية يصعُب قرصنتها.	4,10	,665	05	مرتفعة
10	يُتيح لي البنك إمكانية تغيير الرقم السري عند الحاجة.	4,55	,575	02	مرتفعة
11	ليس بإمكان أي شخص الولوج إلى حسابي الإلكتروني قصد الاطلاع على بياناتي ومعلوماتي.	4,30	,611	03	مرتفعة
	سرية البيانات (Confidentiality):	**4,41**	**,622**	**01**	**مرتفعة**
12	الخدمات الإلكترونية للبنك متاحة باستمرار لمدة 24 ساعة في اليوم وخلال كل أيام الأسبوع.	4,46	,562	01	مرتفعة
13	خدمات المصرف متاحة في كل مكان.	1,78	1,182	05	منخفضة
14	يتيح البنك امكانية الولوج الإلكتروني إلى بياناتي لتدقيقها في أي وقت.	4,18	,837	04	مرتفعة
15	يوفر البنك مجموعة متنوعة من وسائل الاتصال به بصفة دائمة مثلا: Internet-Mobile-Fax-Mail-SMS	4,39	,899	03	مرتفعة
16	من خلال تعاملاتي السابقة بالبطاقة الإلكترونية، لم يسبق لي وأن صادفت خلل في الجهاز ما أدى إلى انقطاع الخدمة.	4,41	,865	02	مرتفعة
	التوافر والديمومة (Availability):	**3,84**	**,710**	**04**	**مرتفعة**
17	يقوم البنك بتوثيق وتسجيل جميع تعاملاتي الإلكترونية بصفة تلقائية.	4,69	,507	03	مرتفعة

18	يمكنني مراجعة وتقفي جميع مسارات المعاملات الإلكترونية التي قمت بها ومعرفة تاريخها وتوقيتها.	4,74	,438	02	مرتفعة
19	يشعرني البنك بالعمليات التي أقوم بها، كسحب الرصيد، التحويلات، الخصم، الدفع، وغير ذلك.	2,61	1,367	05	متوسطة
20	تقوم آلة الموزع الآلي بسحب بطاقتي الإلكترونية تلقائيا عند استعمالها بشكل خاطئ باستمرار.	4,91	,290	01	مرتفعة
21	يتم تجميد حسابي في حال فقدان البطاقة.	3,78	,556	04	مرتفعة
	تتبع الأثر (Traceability):	**4,14**	**,731**	**03**	**مرتفعة**
22	يقدم البنك خدماته بمعدات وأجهزة تقنية متطورة.	4,25	,620	04	مرتفعة
23	أنظمة البنك وأجهزته تعمل بدقة دون أي خلل.	4,38	,566	03	مرتفعة
24	نسبة الأخطاء في نظام المعلومات الخاص بمعاملاتي الإلكترونية مع البنك معدومة بشكل عام.	4,46	,500	02	مرتفعة
25	البنك يستخدم تكنولوجيا بمعايير دولية في إدارة وحماية شبكات الاتصال والبطاقات الإلكترونية.	4,09	1,046	05	مرتفعة
26	عمليات بطاقة الدفع أو السحب الإلكترونية تتم بسرعة عالية وهي توفر لي الجهد والوقت.	4,68	,480	01	مرتفعة
	التكنولوجيا المستخدمة(TechnologyUsed):	**4,37**	**,755**	**02**	**مرتفعة**
27	أثناء تعاملي مع البنك يطلب مني الإدلاء فقط بالمعلومات التي أقبل الإفصاح عنها.	3,25	,913	05	متوسطة
28	بياناتي الشخصية محفوظة في بطاقة الدفع الإلكترونية وسليمة المحتوى ويمكنني تعديلها في حال احتجت ذلك.	4,31	,795	03	مرتفعة
29	يحرص البنك على عدم نشر أو بَث بياناتي الشخصية.	4,55	,697	02	مرتفعة
30	البنك يحترم خصوصية بياناتي الشخصية ولا يشاركها مع أطراف أخرى.	4,57	,695	01	مرتفعة

31	البنك يحمي ويحافظ على بياناتي الشخصية والمعلومات التي جمعها عني ولا أتوقع يوما أن يُتاجر بها.	3,96	,973	04	مرتفعة
	احترام الخصوصية (Privacy):	**3,52**	**,714**	**05**	**متوسطة**

المصدر: من اعداد الطالب اعتمادا على معطيات برنامج spss v26

أعطت نتائج التحليل الاحصائي نتائج **أبعاد الأمن السيبراني** التي تم تقسيمها إلى خمس فقرات كما يلي:

1.1 سرية البيانات: العبارات من 07 إلى 11

تشير النتائج المستخرجة من برنامج التحليل الاحصائي، إلى أن بعد سرية البيانات احتل الصدارة في الأمن السيبراني حيث أن المتوسط الحسابي لهذا البعد كان (مرتفعا) بلغت درجته: 4,41 بانحراف معياري قدره: ,622 وقد احتلت العبارة رقم 07 المتضمنة (يحرص البنك على إعطائي رقما سريا خاصا للبطاقة الإلكترونية منذ يوم التسليم) أعلى متوسط حسابي 4,90 بانحراف معياري قدره: ,304 حيث يرى المستجوبين أن عملية استلامهم لبطاقاتهم الإلكترونية من أول وهلة، يعطي لها البنك أهمية جد بالغة من خلال منحهم رقما سريا خاصا بها، وهي طريقة جيدة من البنك لجعل العملاء يشعرون بحرصه على ضمان سرية بياناتهم والتأكيد على تدابير حمايتها، وقد بلغت جميع العبارات المتبقية لهذا البعد متوسطات حسابية مرتفعة، جاء في المرتبة الثانية العبارة رقم 10 التي نص على: (يتيح لي البنك إمكانية تغيير الرقم السري عند الحاجة) بمتوسط حسابي 4,55 وانحراف معياري قدره: ,575 وفي الأخير احتلت العبارة رقم 09 (الرقم السري لبطاقتي الإلكترونية يصعب قرصنته) المرتبة الأخيرة بمتوسط حسابي 4,10 وبانحراف معياري قدره: ,655 لتعزز نفس الاستنتاج السابق.

2.1 التوافر والديمومة: العبارات من 12 إلى 16

تبين النتائج المعطاة من برنامج التحليل الاحصائي أن مستوى التوافر والديمومة في الأمن السيبراني كان (مرتفعا) إذ بلغت درجة المتوسط الحسابي للبعد: 3,84 بانحراف معياري قدره: ,710 وبذلك يحتل المرتبة الرابعة في أبعاد الأمن السيبراني، حيث كانت درجة المتوسط الحسابي للعبارة رقم 12 الأعلى: 4,46 وبانحراف معياري: ,768 حيث يرى المستجوبين أن الخدمات الإلكترونية المصرفية متوفرة ومتاحة باستمرار لمدة 24 ساعة في اليوم وخلال كل أيام الأسبوع، يمكن إرجاع ذلك إلى تمكنهم من الخدمة باستعمال البطاقات المصرفية الإلكترونية التي تعمل بواسطة أجهزة مختلفة سواء جهاز نهائي الدفع الإلكتروني TPE أو الشباك الآلي للبنك GAB أو الموزع الآلي للأوراق النقدية DAB، لتحتل المرتبة الثانية العبارة رقم 16 (من خلال تعاملاتي السابقة بالبطاقة الإلكترونية، لم يسبق لي وأن صادفت عطل أو خلل في الجهاز ما أدى إلى انقطاع الخدمة) بمتوسط حسابي 4,41 وانحراف معياري ,865 دلالة على سلامة تقديم الخدمة من قبل البنك وتمكنه من المحافظة باستمرار على أمن معاملاته الإلكترونية، إضافة إلى أن أجهزته هي تعمل بصفة تكاملية ومنسجمة فيما بينها دون

حدوث أي مشاكل من شأنها تعطيل الخدمة، ويتب في نفس هذا السياق العبارة رقم 15 (يوفر البنك مجموعة متنوعة من وسائل الاتصال به بصفة دائمة مثلا: sms-internet-mobile-fax-Mail) بمتوسط حسابي مرتفع 4,39 وانحراف معياري قدره: 899, يظهر من خلاله تمكن العملاء من الاتصال المباشر أو غير المباشر بالبنك وفي أي وقت، وجاءت في الأخير العبارة رقم 13 (خدمات المصرف متاحة في كل مكان) بمتوسط حسابي منخفض 1,78 وانحراف معياري قدره: 1,182 يتبين من خلالها عدم الانتشار الواسع لأجهزة نهائي الدفع الإلكتروني TPE، حيث أن استعمالها بولاية غرداية لا يزال حديثا مما يجعل الخدمة المصرفية الإلكترونية لبنك التنمية المحلية غير متوفرة بأوسع نطاق خاصة لدى المحلات التجارية بمختلف أنواعها.

2.2 تتبع الأثر: العبارات من 17 إلى 21

أسفرت نتائج التحليل الاحصائي لبيانات الدراسة المجمعة من الاستبانة، أن تتبع الأثر لبعد الأمن السيبراني احتل المرتبة الثالثة، حيث كان المتوسط الحسابي العام له: 4,14 درجته (مرتفعة) وبانحراف معياري قدره: 731, فكانت استجابة العينة للعبارة رقم 20 التي نص على (تقوم آلة الموزع الآلي بسحب بطاقتي الإلكترونية تلقائيا عند استعمالها بشكل خاطئ باستمرار) بمتوسط حسابي (مرتفع) قدره: 4,91 وانحراف معياري بلغ: 290, كون أن المستجيب يرى أن هاته الخدمة تسمح له بضمان عدم قيام أي شخص دونه باستخدام بطاقته الإلكترونية سواء بعد تعرضها للسرقة أو الضياع بمحاولة سحب الأموال سواء من خلال تجريب أرقام سرية بشكل عفوي أو بشكل خاطئ، وتعكس هذه العملية مدى توفر عنصر تتبع الأثر في الأمن السيبراني للبنك، كما نستنتج أن معظم المستجوبين هم يعلمون بهاته التقنية حيث سبق لهم وأن حدثت لهم أو لغيرهم، تليها استجابة العينة للعبارة رقم 18 التي تنص على (يمكنني مراجعة وتقفي جميع مسارات المعاملات الإلكترونية التي قمت بها ومعرفة تاريخها وتوقيتها) بمتوسط حسابي (مرتفع) قدره: 4,74 وانحراف معياري: 438, تظهر من خلالها تمكين البنك العملاء بتقفي وتتبع مسار مختلف عملياتهم الإلكترونية التي قاموا بها، وهذا بالاطلاع على رصيدهم أو الاطلاع على المبالغ المسحوب أو المدفوعة من وإلى حساباتهم البنكية ومعرفة تواريخها ومواقيتها بالتدقيق، أما إجابة العبارة رقم 19 (يشعرني البنك بالعمليات التي أقوم بها كسحب الرصيد، التحويلات، الخصم، الدفع، وغير ذلك) متوسطها الحسابي 2,61 وانحرافها المعياري 1,367 بدرجة (متوسطة) جاءت في المرتبة الأخيرة، وبهذا تبين لنا أن غالبية المستجوبين لم يستفيدوا من هذه الخدمة كون هاته العملية لا تتأتى للعميل إلا إذا طلب من البنك تمكينه من ذلك.

2.3 التكنولوجيا المستخدمة: العبارات من 22 إلى 26

أظهرت نتائج التحليل الاحصائي، أن التكنولوجيا المستخدمة في بعد الأمن السيبراني كانت الثانية بعد بُعد سرية البيانات بمتوسط حسابي عام (مرتفع) قدره: 4,37 وبانحراف معياري قدره: 755, حيث بلغت جميع أسئلة هذا البعد متوسطات حسابية مرتفعة، بداية من العبارة رقم 26 التي نص على (عمليات بطاقة الدفع

أو السحب الإلكترونية تتم بسرعة عالية وهي توفر لي الجهد والوقت) بمتوسط حسابي قدره: 4,68 وبانحراف معياري: 480, يعني أن المستجوبين راضين عن خدمات البنك الإلكترونية باستخدامهم لنهائي الدفع الإلكتروني TPE والشباك الآلي GAB والموزع الآلي للأوراق النقدية DAB وغيرها، فهي خدمات ذاتية يقوم العميل بخدمة نفسه بنفسه مستعملا بطاقة إلكترونية، خاصة وأننا في عصر السرعة الأمر الذي يحتم على مختلف المؤسسات تسهيل وتسريع تقديم الخدمات بمختلف الطرق التقنية الحديثة وتفادي الطوابير والانتظار والجهد الاضافي، لتحتل المرتبة الثانية العبارة رقم: 24 (نسبة الأخطاء في نظام المعلومات الخاص بمعاملاتي الإلكترونية مع البنك معدومة بشكل عام) بمتوسط حسابي 4,46 وانحراف معياري 500, فالعملاء يؤكدون توفر البنك على تكنولوجيا متطورة بأنظمة دقيقة تعمل بانسجام دون أخطاء أو تكاد تنعدم، وهذا ما تم تأكيده أيضا في العبارة رقم: 25 (البنك يستخدم تكنولوجيا بمعايير دولية في إدارة وحماية شبكات الاتصال والبطاقات الإلكترونية) بمتوسط حسابي 4,09 وانحراف معياري 1,046 يعني تمكين البنك محل الدراسة عملائه من استخدام بطاقات إلكترونية دولية كبطاقة فيزا كارد (VISA Card) وماستر كارد (Master Card) وبطاقة الكوربورايت (Corporate).

5.1 احترام الخصوصية: العبارات من 27 إلى 31

ما يمكن ملاحظته ابتداء من نتائج التحليل الاحصائي أن بعد احترام الخصوصي في الأمن السيبراني حظي بأضعف نسبة حيث بلغ المتوسط الحسابي العام درجة (متوسطة) بمتوسط حسابي: 3,52 وانحراف معياري قدره: 714, وقد احتلت العبارة رقم: 30 (البنك يحترم خصوصية بياناتي الشخصية ولا يشاركها مع أطراف أخرى) المرتبة الأولى بمتوسط حسابي قدره: 4,57 وانحراف معياري قدره: 695, ذلك أن المستجوبين يرون أن البنك محل الدراسة يهتم بحماية بياناتهم الشخصية ويحرص على احترام خصوصيتهم بداية من تسليمهم رقم سري للبطاقة الإلكترونية دون الاطلاع عليه كون البطاقة يتم تصنيعها من قبل شركة SATIM مع تمكين العميل بتغيير رقمه السري مباشرة بعد الاستلام، وهذا ما تم تأكيده في العبارة رقم: 31 (البنك يحمي ويحافظ على بياناتي الشخصية والمعلومات التي جمعها عني ولا أتوقع يوما أن يتاجر بها) بمتوسط حسابي: 3,96 وانحراف معياري: 814, في حين احتلت المرتبة الأخيرة وبدرجة (متوسطة) العبارة رقم: 27 (أثناء تعاملي مع البنك يطلب مني الإدلاء فقط بالمعلومات التي أقبل الإفصاح عنها) بمتوسط حسابي قدره: 3,25 وبانحراف معياري قدره: 913, ما يفسر أن بعض العملاء غير راضين عن بعض المعلومات التي يطلبها منهم البنك، على سبيل المثال لا الحصر ما يتعلق بالتصريح برأس المال، مشاريع العميل الأخرى، عناوين الإقامات المختلفة للعميل، رقم هاتف النقال خاصة فئة الإناث...إلخ.

ولما سبق، باستخدام المتوسطات الحسابية الترتيبية لأبعاد الأمن السيبراني نجد ما يلي:

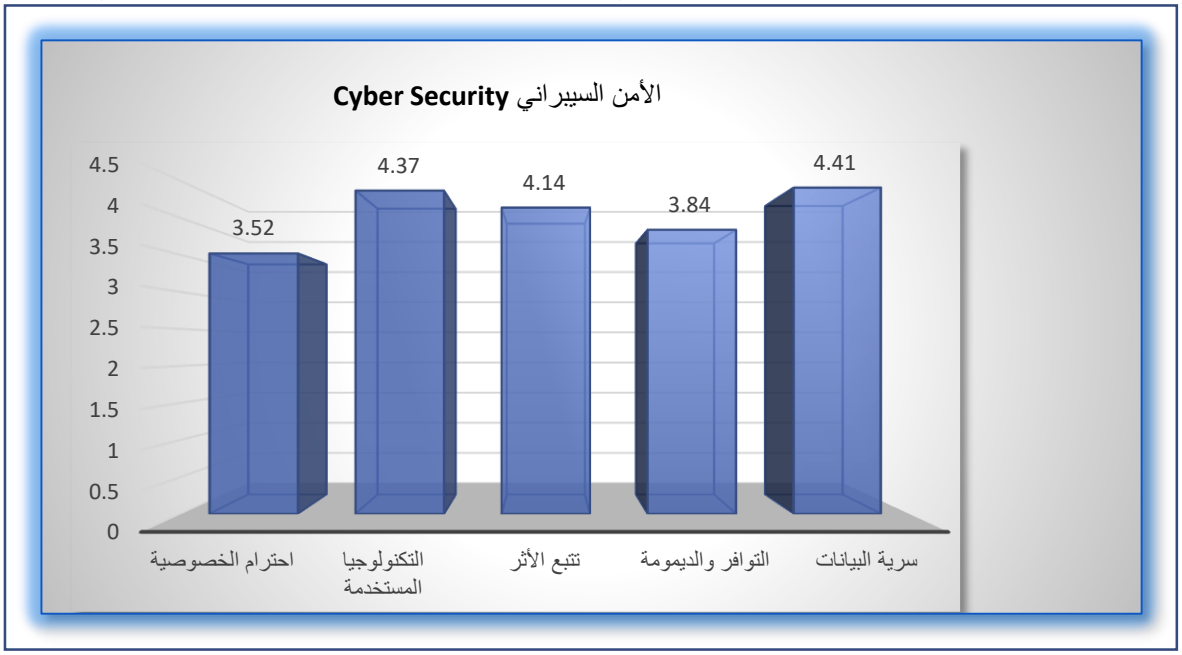
الجدول رقم (IV–8): ترتيب المتوسطات الحسابية والانحرافات المعيارية لأبعاد الأمن السيبراني

	المتوسط الحسابي	الدرجة	الانحراف المعياري	الترتيب
سرية البيانات	4,41	مرتفعة	,622	01
التوافر والديمومة	3,84	مرتفعة	,710	04
تتبع الأثر	4,14	مرتفعة	,731	03
التكنولوجيا المستخدمة	4,37	مرتفعة	,755	02
احترام الخصوصية	3,52	متوسطة	,714	05

المصدر: من اعداد الطالب اعتمادا على معطيات البرنامج spss v26

وفيما يلي تمثيل بياني للمتوسطات الحسابية أبعاد الأمن السيبراني:

الشكل رقم (IV–7): التمثيل البياني للمتوسطات الحسابية لأبعاد الأمن السيبراني



المصدر: من اعداد الطالب اعتمادا على معطيات البرنامج Excel

المطلب الثاني: عرض وتحليل نتائج أبعاد المتغير الوسيطي

عرض وتحليل نتائج المتغير الوسيطي "ثقة العملاء" كانت كما يلي:

1. الإجابة عن السؤال الثاني:

- **ما درجة الثقة لدى العملاء؟**

للإجابة على السؤال الثاني، قام الطالب بحساب المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد العينة من المستهلكين الالكترونيين، وقد بينت نتائج المعالجة الاحصائية ما يلي:

الجدول رقم (IV–9): المتوسطات الحسابية والانحرافات المعيارية لفقرات محور ثقة العملاء

الرقم	السؤال	المتوسط الحسابي	الانحراف المعياري	الترتيب	الدرجة
32	أثق بجوانب الأمان المتعلقة باستخدام الخدمات الإلكترونية المصرفية.	4,39	,676	01	مرتفعة
33	البنك الذي أتعامل معه لديه القدرة والكفاءة في تقديم خدماته المصرفية الإلكترونية التي أحتاجها.	2,31	,723	05	منخفضة
34	البنك لديه خبرة كافية لأداء الخدمات الإلكترونية بكل فعالية والتزام.	4,06	,810	04	مرتفعة
35	سياسة البنك وقوانينه الموجودة حاليا توفر لي الحماية عند استخدام الخدمات الإلكترونية المصرفية.	4,23	,781	03	مرتفعة
36	البنك يتعامل بكل مصداقية وإخلاص.	4,25	,780	02	مرتفعة
	البعد المعرفي (Cognitive Dimension)	**3.84**	**,754**	**02**	**مرتفعة**
37	أشعر بالأمان في اعتمادي التعامل إلكترونيا مع البنك.	4,30	,647	02	مرتفعة
38	أعتقد أن البنك يريد لي الأفضل من خلال تعاملاتي الإلكترونية معه.	4,11	,706	04	مرتفعة
39	البنك يأخذ بعين الاعتبار مصلحتي واهتمامي من خلال نفعي بالخدمات الإلكترونية المصرفية بأفضل طريقة.	2,34	,939	05	متوسطة
40	أرى أن البنك يبذل العناية والجهد اللازم من أجل حماية بياناتي الشخصية.	4,22	,738	03	مرتفعة
41	يستجيب البنك بسرعة لحل أي مشكلة تصادفني تتعلق بسلامة وأمن البطاقة الإلكترونية.	4,41	,622	01	مرتفعة
	البعد العاطفي (Emotional Dimension)	**3,87**	**,730**	**01**	**مرتفعة**

المصدر: من اعداد الطالب اعتمادا على معطيات البرنامج spss v26

1.1 نتائج التحليل الاحصائي للمتغير الوسيطي "الثقة" الأسئلة من 31 إلى 36:

أعطت نتائج التحليل الاحصائي نتائج **أبعاد ثقة العملاء** التي تم تقسيمها إلى فقرتين كما يلي:

1.2 البعد المعرفي: العبارات من 32 إلى 36

تشير النتائج المستخرجة من برنامج التحليل الاحصائي لاستجابة المبحوثين، إلى أن البعد المعرفي في ثقة العملاء احتل المرتبة الثانية بعد البعد العاطفي، حيث سجل المتوسط الحسابي العام: 3,84 بانحراف معياري: 754, بدرجة (مرتفعة) مما يجعل للبعد أهمية كمتغير وسيط في النموذج العام للدراسة، حيث احتلت إجابات العبارة رقم: 32 أعلى متوسط حسابي بدرجة (مرتفعة) قدره: 4,39 وانحراف معياري قدره: 676, مضمونه (أثق بجوانب الأمان المتعلقة باستخدام الخدمات الإلكترونية المصرفية) مما يدل على أن الثقة المعرفية للمستجوبين تكون كبيرة وتزداد أكثر من خلال التدابير والإجراءات الأمنية والتنظيمية التي ينتهجها البنك لحماية العملاء من المخاطر والتهديدات السيبرانية في مختلف التعاملات المصرفية الإلكترونية، تلاه المتوسط الحسابي للعبارة رقم 36 (البنك يتعامل بكل مصداقية وإخلاص) حيث بلغ المتوسط الحسابي: 4,25 وهي درجة مرتفعة وانحراف معياري قدره: 780, ما يعكس ردة فعل إيجابية للعملاء تجاه البنك من خلال الحكم عليهم بالتفان والإخلاص في تقديم الخدمة، وهذا ما يعزز الثقة المعرفية لهم، في حين بلغ المتوسط الحسابي للعبارة رقم: 35 (سياسة البنك وقوانينه الموجودة حاليا توفر لي الحماية عند استخدام الخدمات الإلكترونية المصرفية) بمتوسط حسابي قدره: 4,23 وبانحراف معياري قدره:781, أما العبارة رقم: 33 (البنك الذي أتعامل معه لديه القدرة والكفاءة في تقديم الخدمات المصرفية التي أحتاجها) احتلت المرتبة الخامسة والأخيرة بدرجة (منخفضة) بمتوسط حسابي: 2,31 وانحراف معياري قدره: 723, ما يفسر تلقي العملاء مجموعة خدمات مصرفية إلكترونية بكيفية لا تلبي جميع حاجاتهم ورغباتهم وبهذا هي ليست كافية، كون عميل اليوم يتطلع لما تقدمه البنوك الإلكترونية في الدول الأوروبية والأمريكية أو حتى الخليجية من خدمات متنوعة ومختلفة وفي شتى المجالات، بينما الخدمات الإلكترونية المصرفية المقدمة من قبل البنك محل الدراسة هي تنحصر في بعض المجالات فقط.

2.2 البعد العاطفي: العبارات من 37 إلى 41

أسفرت نتائج التحليل الاحصائي، إلى أن البعد العاطفي في ثقة العملاء احتل الصدارة حيث سجل المتوسط الحسابي العام قيمة (مرتفعة) قدرتـــ: 3,87 وانحراف معياري قدره: 730, مما يجعل أيضا للبعد أهمية كمتغير وسيط في النموذج العام للدراسة، حيث احتلت إجابات العبارة رقم: 41 أعلى متوسط حسابي بدرجة (مرتفعة) قدره: 4,41 وانحراف معياري قدره: 622, مضمونه (يستجيب البنك لحل أي مشكلة تصادفني تتعلق بسلامة وأمن البطاقة الإلكترونية) مما يدل على أن الثقة العاطفية للعملاء تكون كبيرة وتزداد أكثر حين يستجيب البنك لمعالجة مشاكلهم أثناء تقديمه للخدمات، خاصة ما تعلق منها بالأمن والسلامة الرقمية كون هاته المعاملات مالية ومنها ما يمس بالخصوصية، تلاه المتوسط الحسابي للعبارة رقم: 37 (أشعر بالأمان في اعتمادي التعامل إلكترونيا مع البنك) حيث بلغ المتوسط الحسابي: 4,30 وهي درجة (مرتفعة) وانحراف معياري قدره: 647, ما يفسر شعور العميل بالأمان في التعامل الإلكتروني بدل التقليدي هو توفر عنصر الموثوقية من

خلال انعدام حدوث المشاكل الأمنية التي تمس المعاملات الإلكترونية بصفة عامة، في حين بلغ المتوسط الحسابي للعبارة رقم: 40 (أرى أن البنك يبذل العناية والجهد اللازم من أجل حماية بياناتي الشخصية) بمتوسط حسابي قدره: 4,22 وبانحراف معياري قدره: 738, هنا تظهر ثقة العميل في البنك من خلال اعترافه له ببذل الجهد اللازم بغية حمايته من المخاطر، ولا يتأتى هذا إلا بملاحظته ذلك أو معايشته للتدابير والإجراءات الأمنية المتخذة من قبل البنك ميدانيا، أما العبارة رقم: 39 (البنك يأخذ بعين الاعتبار مصلحتي واهتمامي من خلال نفعي بالخدمات الإلكترونية المصرفية بأفضل طريقة) احتلت المرتبة الأخيرة بدرجة (متوسطة) وبمتوسط حسابي قدره: 2,34 وانحراف معياري قدره:939, ويمكن تفسير ذلك كما فسرناه سابقا أن العميل اليوم يقارن ما يتلقاه من خدمات مصرفية إلكترونية بالبنك محل الدراسة، بتلك التي يتلقاها العميل في الدول الأجنبية، حيث أصبحت حاجاته ورغباته تتطلع لمجالات أخرى غير مشبعة.

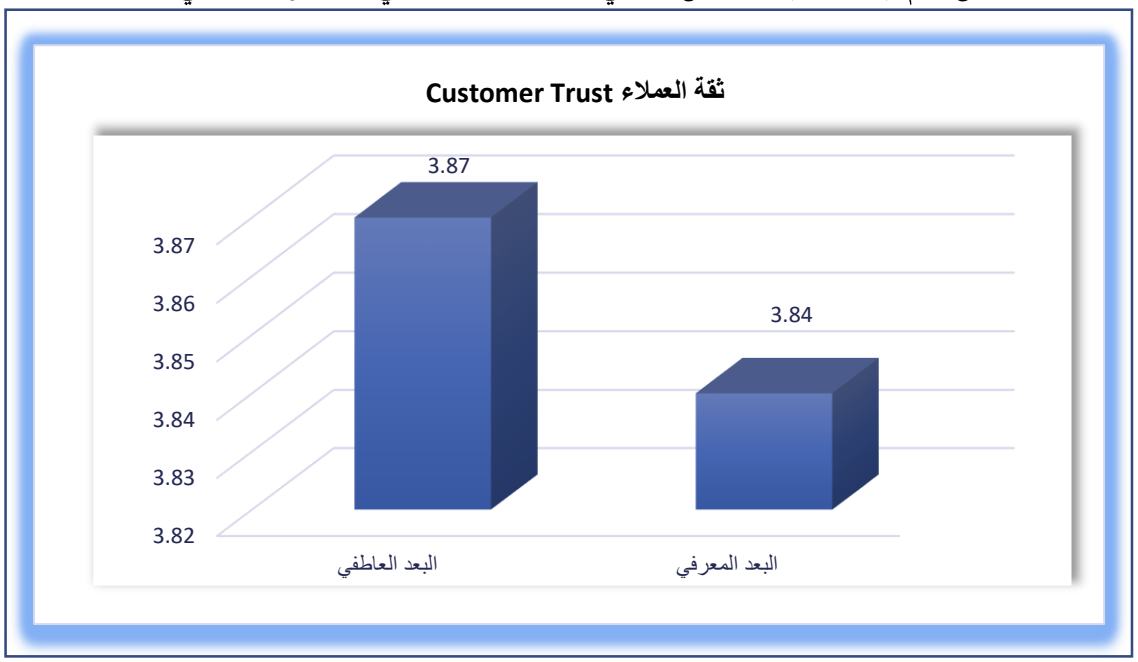
يوضح الجدول والشكل البياني التاليين ترتيب المتوسطات الحسابية والانحرافات المعيارية لأبعاد ثقة العملاء:

الجدول رقم (IV–9): ترتيب المتوسطات الحسابية والانحرافات المعيارية لأبعاد ثقة العملاء

	المتوسط الحسابي	الدرجة	الانحراف المعياري	الترتيب
البعد المعرفي	3,84	مرتفعة	,754	02
البعد العاطفي	3,87	مرتفعة	,730	01

المصدر: من اعداد الطالب اعتمادا على معطيات البرنامج spss v26

الشكل رقم (IV–8): التمثيل البياني للمتوسط الحسابي للمتغير الوسيطي "الثقة"



المصدر: من اعداد الطالب اعتمادا على معطيات البرنامج Excel

المطلب الثالث: عرض وتحليل نتائج المتغير التابع

عرض وتحليل نتائج المتغير التابع "الخدمات الإلكترونية المصرفية" كانت كما يلي:

1. الإجابة على السؤال الثالث:

- **ما درجة استخدام الخدمات الإلكترونية المصرفية؟**

بينت نتائج المعالجة الاحصائية لاستجابة أفراد العينة لفقرات المتغير التابع "الخدمات الإلكترونية المصرفية"، وخاصة المتوسطات الحسابية والانحرافات المعيارية للفقرات ما يلي:

الجدول رقم (IV-11): المتوسطات الحسابية والانحرافات المعيارية لفقرات الخدمات الإلكترونية المصرفية

الرقم	السؤال	المتوسط الحسابي	الانحراف المعياري	الترتيب	الدرجة
37	الخدمات الإلكترونية المصرفية أفضل بكثير من الخدمات المصرفية التقليدية وهي تلبي متطلباتي.	4,43	,492	01	مرتفعة
38	تشجعني السياسة الأمنية للبنك الخاصة باستعمال البطاقات الإلكترونية على استمرارية التعامل معه.	4,33	,578	03	مرتفعة
39	درجة اهتمام البنك بأمن بياناتي الشخصية المتعلقة بالخدمات الإلكترونية المصرفية تجعلني في ثقة وارتياح.	4,42	,545	02	مرتفعة
40	البنك يحمي ويؤمّن بياناتي الشخصية أثناء استخدام الخدمات الإلكترونية المصرفية أكثر مما توقعت.	2,30	1,641	05	منخفضة
41	سوف أوصي الآخرين باستخدام الخدمات الإلكترونية المصرفية.	4,31	,616	04	مرتفعة
	الخدمات الإلكترونية المصرفية (Electronic Banking Services)	**3,95**	**,774**		**مرتفعة**

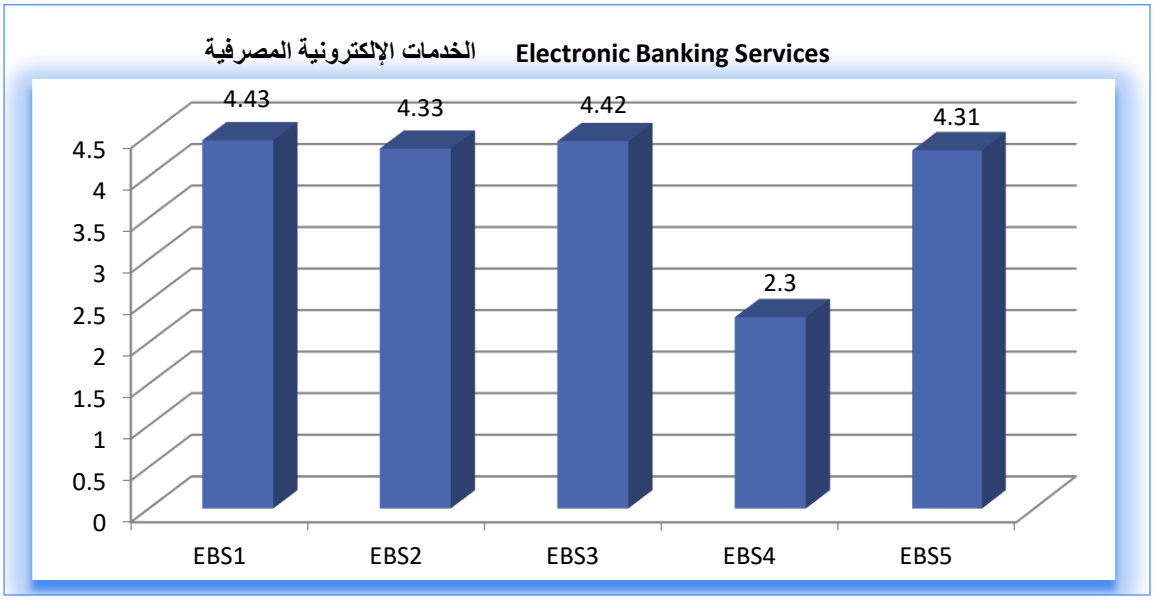
المصدر: من اعداد الطالب اعتمادا على معطيات البرنامج spss v26

1.1 نتائج التحليل الاحصائي للمتغير التابع " الخدمات الإلكترونية المصرفية": العبارات من 42 إلى 46

يتضح من خلال نتائج الجدول رقم (IV-11)، أن درجة المتوسط الحسابي العام لبعد الخدمات الإلكترونية المصرفية كان (مرتفعا) إذ بلغت 3,95 وانحراف معياري قدره: ,774 حيث كانت أعلى درجة لإجابة العبارة رقم: 37 (الخدمات المصرفية الإلكترونية أفضل بكثير من الخدمات المصرفية التقليدية وهي تلبي متطلباتي)

بمتوسط حسابي (درجته مرتفعة): 4,43 وبانحراف معياري: 492, مما يؤكد أن العميل راض عن الخدمة البنكية الإلكترونية مقارنة بما كان يتلقاه أيام التقليدي، نظرا لما وفرته من راحة ووقت وسهولة استخدام، تلته إجابات العبارة رقم: 39 التي تنص على (درجة اهتمام البنك بأمن بياناتي الشخصية المتعلقة بالخدمات الإلكترونية المصرفية تجعلني في ثقة وارتياح) بمتوسط حسابي: 4,42 وانحراف معياري: 545, وهي درجة مرتفعة أيضا، لتكون إجابة العبارة رقم: 38 (تشجعني السياسة الأمنية للبنك الخاصة باستعمال البطاقات الإلكترونية على استمرارية التعامل معه) في المرتبة الثالثة بمتوسط حسابي درجته (مرتفعة) قدره: 4,33 وانحراف معياري قدره: 578, حيث بينت القدرة العالية للبنك في حماية تحقيق سياسة أمنية ناجحة من خلال تأمين وحماية بيانات العملاء رغم مخاطر وتهديدات عالم الافتراض، وبهذا فالعميل أجاب بقبول استمراريته في التعامل مع البنك إلكترونيا، لتكون نتائج العبارة رقم: 41 (سوف أوصي الآخرين باستخدام الخدمات الإلكترونية المصرفية) بمتوسط حسابي قدره: 4,31 وانحراف معياري:616, تعكس مستوى رضا العميل ومدى استعداده لتشجيع الآخرين بالكلمة المنطوقة نحو التعامل مع البنك محل الدراسة، أما عن إجابات العبارة الأخيرة رقم: 40 (البنك يحمي ويؤمن بياناتي الشخصية أثناء استخدام الخدمات الإلكترونية المصرفية أكثر مما توقعت) جاء بمتوسط حسابي درجته (منخفضة): 2,30 وانحراف معياري قدره: 1,641 يدل ذلك على توافق ما توقعه العميل سابقا وما تحقق حاضرا من البنك محل الدراسة دون تجاوز توقعاته.

الشكل رقم (IV–9): التمثيل البياني للمتوسط الحسابي للمتغير التابع الخدمات الإلكترونية المصرفية



المصدر: من اعداد الطالب اعتمادا على معطيات البرنامج Excel

المبحث الثالث: اختبار الفرضيات ومناقشة النتائج

بعد استيفاء متطلبات الجودة والكفاءة في نموذج الدراسة العام على مستوى نموذج القياس والنموذج الهيكلي، يتم من خلال هذا المبحث استكمال مسار تحليل واختبار الفرضيات ومن ثم الإجابة على تساؤلات البحث، وعليه تم تقسيم المبحث إلى ثلاث مطالب على النحو التالي:

-معاملات المسار لمتغيرات الدراسة.

-اختبار الفرضيات.

-تفسير ومناقشة النتائج.

المطلب الأول: معاملات المسار لمتغيرات الدراسة

بغرض اختبار الفرضيات وعملا بمنهجية النمذجة الهيكلية بطريقة المربعات الصغرى الجزئية، يتم من خلال البرنامج الاحصائي (Smart PLS.4) تحديد معاملات المسارات المحددة في نموذج الدراسة.

1. معاملات المسارات (Path Coefficients)

تمهيدا لعملية اختبار الفرضيات، يتم تحديد معاملات المسارات لقياس الأثر بين المتغيرات، وحساب قيم الاحتمالات لاختبار الدلالة الاحصائية في العلاقات بين متغيرات الدراسة، عبر التقنية الحديثة المسماة اختصارا (Bootstrapping) التي تعني المعاينة مع الاستبدال، التي يوفرها التطبيق البرمجي الاحصائي المستخدم في هذه الدراسة (Smart PLS.4)[1]

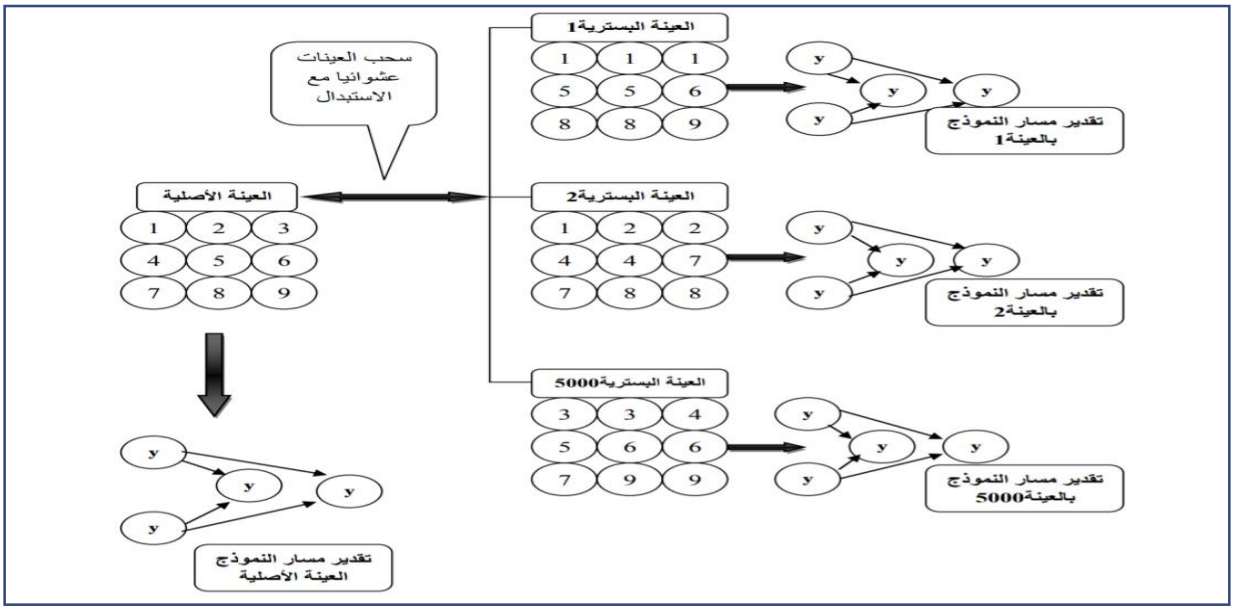
2. تقنية المعاينة مع الاستبدال (Bootstrapping):

تمثل تقنية البوتسراب الأسلوب الاحصائي الحسابي للحصول على تقديرات دقيقة، بناء على عملية تشكيل غير معلمية، حيث تتم عملية إحلال التوزيعات المعروفة بالتوزيعات الغير معروفة، يتم إنشاء عينات من أجل الحصول على تقديرات في النموذج، حيث تقوم التقنية على فكرة المعاينة بالإرجاع، وذلك من خلال سحب عدد كبير من العينات مع الاستبدال من العينات الأصلية، قد يصل السحب حدود 5000 عينة، حيث تنطوي كل عينة مسحوبة على عدد من الحالات الموجودة في العينة الأصلية، ويتم تقدير نموذج المسار 5000 مرة.[2] والشكل الموالي يوضح طريقة عمل تقنية المعاينة مع الاستبدال:

[1] Sandra Streukens, Sara Leroi Werelds, **Bootstrapping and PLS-SEM / A step by step guide to get more out of your Bootstrap Results**, Europen Management Journal, Vol 34, N 6, 2016, P P 618-632.

[2] Hair Joseph, Hult Tomas, Marko Sarstedt, Hollingsworth**, A Primer on Partial Least Squares Structural Equation Modeling PLS-SEM**, 2ed, Sag, Thousand Oaks, CA 2017, P 152.

الشكل رقم (IV–10): تقنية المعاينة مع الاستبدال (Bootstrapping)



Source: Hair Joseph, et Al, Same Referance as Above, p 152.

يوضح الشكل رقم: (IV–10) مبدأ عمل تقنية المعاينة مع الاستبدال (Bootstrapping)، حيث يقوم البرنامج الحاسوبي بسحب عينة أولى جديدة من العينة الأصلية كل مرة ومن ثم يعمل على تقديرها ضمن مسار النموذج، ويعيد تشكيل عينة ثانية من العينة الأصلية لتقديرها ضمن نموذج الدراسة وهكذا تستمر العملية آليا مع الثالثة والرابعة حتى بلوغ 5000 عينة مشكلة ينتج عنها 5000 عملية تقدير ضمن المسار.

3. نتائج معاملات المسار

باستخدام البرنامج الحاسوبي (Smart PLS.4) وبتقنية التقدير (Bootstrapping) تم الحصول على نتائج معاملات المسارات المكونة للنموذج بين متغيرات الدراسة، ومن خلالها يتم اختبار فرضيات الدراسة مثلما هو مبين في الجدول التالي:

جدول رقم (IV–12): نتائج معامل المسار للعلاقات المباشرة بين متغيرات الدراسة

الإحصاءات / المتغيرات	معامل المسار	معامل R^2	الانحراف المعياري Stqndqrd Deviqtion	قيمة (T) Statistics	قيمة المعنوية P Values
سرية البيانات---->البعد المعرفي للثقة	0.742	0.261	0.01	23.601	0.00
سرية البيانات------>البعد العاطفي للثقة	0.414	0.222	0.01	9.561	0.00
التوافر والديمومة-->البعد المعرفي للثقة	0.641	0.413	0.02	2.763	0.00
التوافر والديمومة-->البعد العاطفي للثقة	-0.201	0.194	0.01	-1.652	0.109
التكنولوجيا المستخدمة>البعد المعرفي للثقة	0.614	0.462	0.01	15.704	0.00

التكنولوجيا المستخدمة>البعد العاطفي للثقة	0.080	0.301	0.01	2.177	0.01
احترام الخصوصية--->البعد المعرفي للثقة	-0.114	0.114	0.01	0.333	0.176
احترام الخصوصية---->البعد العاطفي للثقة	0.204	0.335	0.02	13.919	0.00
تتبع الأثر---------->البعد المعرفي للثقة	0.689	0.225	0.01	2.905	0.00
تتبع الأثر---------->البعد العاطفي للثقة	-0.197	0.311	0.03	30.172	0.209
البعد المعرفي> الخدمات الإلكترونية المصرفية	0.700	0.662	0.02	5.572	0.00
البعد العاطفي> الخدمات الإلكترونية المصرفية	0.060	0.202	0.01	1.976	0.00
سرية البيانات----->الخدمات الإلكترونية المصرفية	0.689	0.214	0.03	5.598	0.00
التوافر والديمومة-------->الخدمات الإلكترونية المصرفية	0.501	0.473	0.01	6.490	0.00
التكنولوجيا المستخدمة--->الخدمات الإلكترونية المصرفية	0.790	0.410	0.01	3.972	0.00
احترام الخصوصية-----> الخدمات الإلكترونية المصرفية	-1.045	0.123	0.01	-1.276	0.304
تتبع الأثر-------> الخدمات الإلكترونية المصرفية	0.496	0.180	0.03	2.089	0.00

المصدر: من اعداد الطالب بناء على مخرجات برنامج Smart PLS.4

يلخص الجدول رقم: (IV-12) النتائج الخاصة بالمسارات والقيم الضرورية لفحص الدلالة الإحصائية، وبناء على ذلك يمكن تفريغ المعطيات في جداول حسب فرضيات الدراسة لتأكيدها أو نفيها.

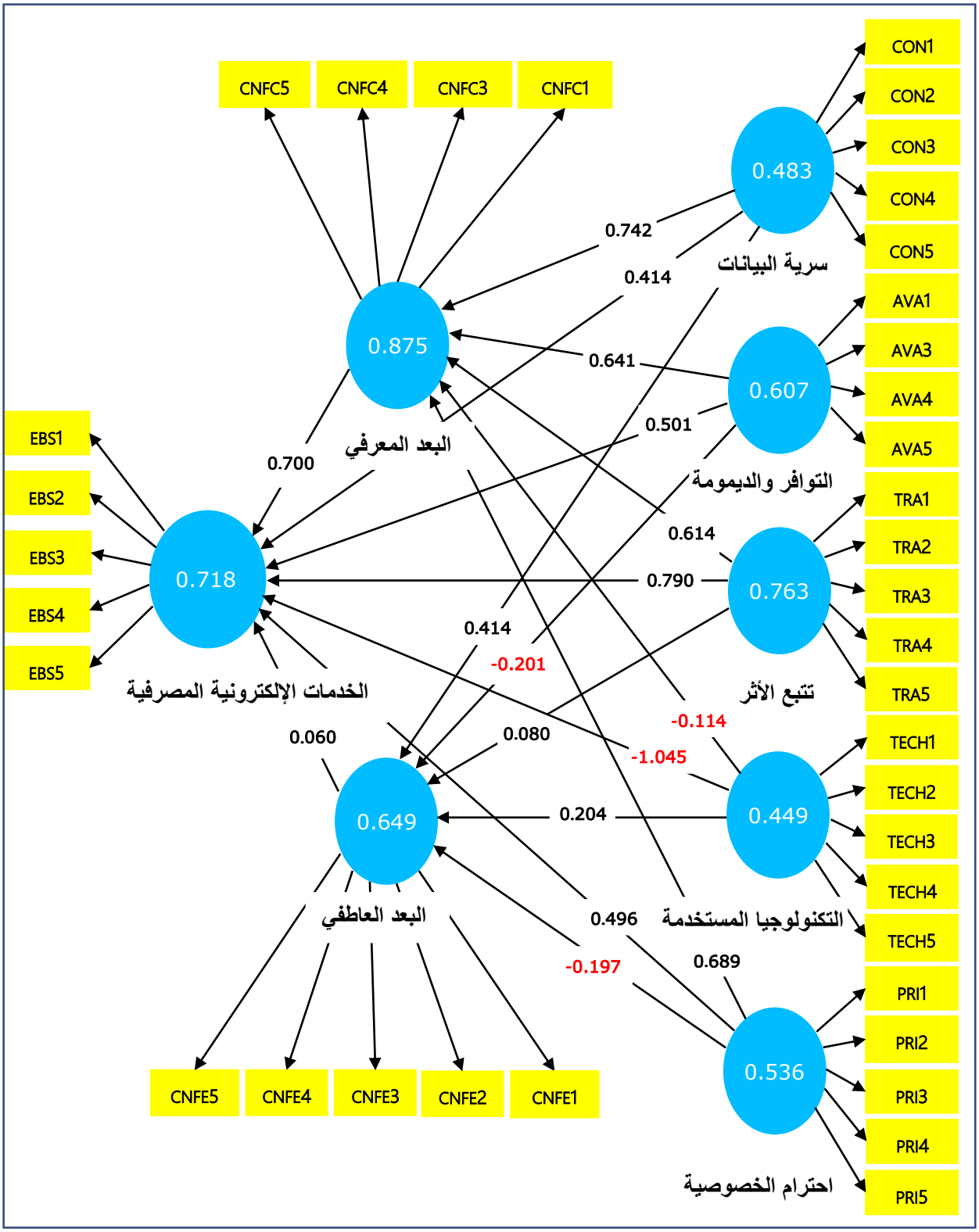
بعد التأكد من عدم وجود التداخل الخطي بين المباني (VIF)، وتقييم ملاءمة معاملات المسار (Path Coefficients)، بالإضافة إلى التأكد من قيم كل من معامل التفسير R^2 وحجم الأثر F^2 سيتم في الموالية اختبار نتائج الفرضيات، حيث تقبل الفرضية إذا تحقق الشرطين معا (أن α دالة إحصائيا، وقيمة $T>1.96$ من عند مستوى الدلالة 5%، أما إذا لم يتحقق أحد الشرطين تقبل الفرضية العدمية.

المطلب الثاني: اختبار فرضيات الدراسة

خصص هذا المطلب في اختبار فرضيات البحث، حيث يتم الاستعانة بالجداول التي تلخص النتائج حسب الفرضيات، فضلا عن الأشكال التوضيحية لمسار العلاقات حسب الفرضيات يرافقها التفسير والتعليق لتبرير وتأكيد أو نفي صحة الفرضيات.

والشكل الموالي رقم: (IV-11) يوضح نموذج مسار العلاقات بين متغيرات الدراسة كما يلي:

الشكل رقم: (IV–11) نموذج مسار العلاقات بين متغيرات الدراسة



المصدر: من اعداد الطالب بناء على مخرجات برنامج Smart PLS.4

أولا: اختبار وتحليل مسار الفرضية الرئيسية الأولى:

- **H1: هناك تأثير مباشر ذو دلالة إحصائية عند مستوى دلالة 0،05 لأبعاد الأمن السيبراني في ثقة العملاء لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.**

وهذه الفرضية جاءت للإجابة على السؤال الفرعي الأول:

1- ما مدى تأثير أبعاد الأمن السيبراني في ثقة العملاء عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية؟

ويمكننا الاستعانة بالفرضيات الفرعية التالية:

- **H1-1: هناك تأثير مباشر بين سرية البيانات والثقة المعرفية للعملاء عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.**
- **H1-2: هناك تأثير مباشر بين التوافر والديمومة والثقة المعرفية للعملاء عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.**
- **H1-3: هناك تأثير مباشر بين التكنولوجيا المستخدمة والثقة المعرفية العملاء عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.**
- **H1-4: هناك تأثير مباشر بين احترام الخصوصية والثقة المعرفية للعملاء عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.**
- **H1-5: هناك تأثير مباشر بين تتبع الأثر والثقة المعرفية للعملاء عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.**
- **H1-6: هناك تأثير مباشر بين سرية البيانات والثقة العاطفية للعملاء عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.**
- **H1-7: هناك تأثير مباشر بين التوافر والديمومة والثقة العاطفية للعملاء عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.**
- **H1-8: هناك تأثير مباشر بين التكنولوجيا المستخدمة والثقة العاطفية للعملاء عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.**
- **H1-9: هناك تأثير مباشر بين احترام الخصوصية والثقة العاطفية للعملاء عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.**
- **H1-10: هناك تأثير مباشر بين تتبع الأثر والثقة العاطفية للعملاء عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.**

يبين الشكل رقم: (IV-11) أن معاملات المسار بين كل من متغير الأمن السيبراني ومتغير ثقة العملاء تشير إلى علاقات تأثير متباينة من بعد إلى أخر، ويمكننا تفصيل النتائج حسب الفرضيات الفرعية التالية:

1.1 اختبار الفرضية الفرعية الأولى:

H1-1: هناك تأثير مباشر بين سرية البيانات والثقة المعرفية للعملاء عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.

يلخص الجدول رقم: (IV-13) مخرجات برنامج (Smart PLS.4) لنتائج تحليل مسار العلاقة بين بعد سرية البيانات والثقة المعرفية للعملاء المتوصل اليها من النموذج العام للدراسة كالتالي:

الجدول رقم (IV-13): نتائج تحليل مسار العلاقة بين بعد سرية البيانات والثقة المعرفية للعملاء

المتغير المستقل	المتغير الوسيط				
	الثقة المعرفية للعملاء				
سرية البيانات	معامل المسار	معامل R^2	قيمة T	مستوى P	النتيجة
	0.742	0.261	23.601	0.00	يوجد تأثير

المصدر: من إعداد الطالب بناء على نتائج برنامج (Smart PLS.4)

من خلال الشكل رقم: (IV-11) والجدول رقم: (IV-13) تشير النتائج إلى أن معامل مسار متغير سرية البيانات على الثقة المعرفية للعملاء قد بلغت قيمته (0.742)، حيث يشر هذا المعامل إلى ارتباط إيجابي قوي جدا بين المتغيرين، في حين أن معامل التحديد R^2 يفيد بأن سرية البيانات تفسر فقط نسبة 26% من التغير في الثقة المعرفية للعملاء، ونسبة 74% الباقية من التغيرات تعود إلى عوامل أخرى، كما تشير النتائج إلى أن القيمة الاحتمالي P بلغت 0.00 وهي أقل من مستوى الدلالة المعتمدة في الدراسة (α=0.05) عند مستوى ثقة 95%، فضلا عن قيمة T المحسوبة التي بلغت (23.601) أكبر من قيمة T الجدولية (1.96)، وهذا يعني وجود أثر ذو دلالة إحصائية.

وبناء على ذلك يتم قبول الفرضية الفرعية الأولى (**H1-1**) الآتية:

هناك تأثير مباشر بين سرية البيانات والثقة المعرفية للعملاء عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.

2. اختبار الفرضية الفرعية الثانية:

H1-2: هناك تأثير مباشر بين التوافر والديمومة والثقة المعرفية للعملاء عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.

يلخص الجدول رقم: (IV-14) مخرجات برنامج (Smart PLS.4) لنتائج تحليل مسار العلاقة بين بعد التوافر والديمومة والثقة المعرفية للعملاء المتوصل إليها من النموذج العام للدراسة كالتالي:

الجدول رقم (IV-14): نتائج تحليل مسار العلاقة بين بعد التوافر والديمومة والثقة المعرفية للعملاء

المتغير المستقل	المتغير الوسيط				
	الثقة المعرفية للعملاء				
التوافر والديمومة	معامل المسار	معامل R^2	قيمة T	مستوى P	النتيجة
	0.641	0.413	2.763	0.00	يوجد تأثير

المصدر: من إعداد الطالب بناء على نتائج برنامج (Smart PLS.4)

من خلال الشكل رقم: (IV-11) والجدول رقم: (IV-14): تشير النتائج إلى أن معامل مسار متغير التوافر والديمومة على الثقة المعرفة للعملاء قد بلغت قيمته (0.641)، حيث يشر هذا المعامل إلى ارتباط إيجابي قوي بين المتغيرين، في حين أن معامل التحديد R^2 يفيد بأن نسبة 41% من التغير في الثقة المعرفية للعملاء يعود إلى تأثير التوافر والديمومة، ونسبة 59% الباقية من التغيرات تعود إلى عوامل أخرى، كما تشير النتائج إلى أن القيمة الاحتمالي P بلغت 0.00 وهي أقل من مستوى الدلالة المعتمدة في الدراسة (α=0.05) عند مستوى ثقة 95%، فضلا عن قيمة T المحسوبة التي بلغت (2.763) أكبر من قيمة T الجدولية (1.96)، وهذا يعني وجود أثر ذو دلالة إحصائية.

وبناء على ذلك يتم قبول الفرضية الفرعية الثانية (**H1-2**) الآتية:

هناك تأثير مباشر بين التوافر والديمومة والثقة المعرفية للعملاء عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.

3. اختبار الفرضية الفرعية الثالثة:

H1-3: هناك تأثير مباشر بين التكنولوجيا المستخدمة والثقة المعرفية للعملاء عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.

يلخص الجدول رقم: (IV-15) مخرجات برنامج (Smart PLS.4) لنتائج تحليل مسار العلاقة بين بعد التكنولوجيا المستخدمة والثقة المعرفية للعملاء المتوصل إليها من النموذج العام للدراسة كالتالي:

الجدول رقم (IV-15): نتائج تحليل مسار العلاقة بين بعد التكنولوجيا المستخدمة والثقة المعرفية للعملاء

المتغير المستقل	المتغير الوسيط				
	الثقة المعرفية للعملاء				
التكنولوجيا المستخدمة	معامل المسار	معامل R^2	قيمة T	مستوى P	النتيجة
	0.614	0.462	15.704	0.00	يوجد تأثير

المصدر: من اعداد الطالب بناء على نتائج برنامج (Smart PLS.4)

من خلال الشكل رقم: (IV-11) والجدول رقم: (IV-15) تشير النتائج إلى أن معامل مسار متغير التكنولوجيا المستخدمة على الثقة المعرفة للعملاء قد بلغت قيمته (0.614)، حيث يشر هذا المعامل إلى ارتباط إيجابي قوي بين المتغيرين، في حين أن معامل التحديد R^2 يفيد بأن نسبة 46% من التغير في الثقة المعرفية للعملاء يعود إلى تأثير التكنولوجيا المستخدمة، ونسبة 54% الباقية من التغيرات تعود إلى عوامل أخرى، كما تشير النتائج إلى أن القيمة الاحتمالي P بلغت 0.00 وهي أقل من مستوى الدلالة المعتمدة في الدراسة (α=0.05) عند مستوى ثقة 95%، فضلا عن قيمة T المحسوبة التي بلغت (15.704) أكبر من قيمة T الجدولية (1.96)، وهذا يعني وجود أثر ذو دلالة إحصائية.

وبناء على ذلك يتم قبول الفرضية الفرعية الثالثة (H1-3) الآتية:

هناك تأثير مباشر بين التكنولوجيا المستخدمة وثقة المعرفية للعملاء عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.

4. اختبار الفرضية الفرعية الرابعة:

H1-4: هناك تأثير مباشر بين احترام الخصوصية والثقة العرفية للعملاء عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.

يلخص الجدول رقم: (IV-16) مخرجات برنامج (Smart PLS.4) لنتائج تحليل مسار العلاقة بين بعد احترام الخصوصية والثقة العرفية للعملاء المتوصل إليها من النموذج العام للدراسة كالتالي:

الجدول رقم (IV-16): نتائج تحليل مسار العلاقة بين بعد احترام الخصوصية والثقة المعرفية للعملاء

المتغير المستقل	المتغير الوسيط				
	الثقة المعرفية للعملاء				
احترام الخصوصية	معامل المسار	معامل R^2	قيمة T	مستوى P	النتيجة
	-0.114	0.114	0.333	0.176	لا يوجد تأثير

المصدر: من اعداد الطالب بناء على نتائج برنامج (Smart PLS.4)

من خلال الشكل رقم: (IV-11) والجدول أعلاه رقم: (IV-16) تظهر النتائج بأن معامل مسار متغير احترام الخصوصية على الثقة المعرفة للعملاء قد بلغت قيمته (0.201-)، ويشر هذا المعامل إلى علاقة ارتباط سلبية متوسطة بين المتغيرين، ومن متابعة قيمة T المحسوبة (1.652-) فهي أقل من قيمة T الجدولية (1.96) والقيمة المعنوية P بلغت 0.109 وهي أكبر من مستوى الدلالة المعتمدة في الدراسة (α=0.05) عند مستوى ثقة 95%، وبهذا فالنتائج هي تشير إلى عدم وجود علاقة ارتباطية موجبة بين متغير احترام الخصوصية والثقة المعرفة للعملاء.

وبناء على ذلك يتم **رفض الفرضية الفرعية الرابعة (H1-4)** وقبول الفرضية الصفرية التالية:

لا يوجد تأثير مباشر بين احترام الخصوصية والثقة المعرفية للعملاء عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.

5.اختبار الفرضية الفرعية الخامسة:

H1-5: هناك تأثير مباشر بين تتبع الأثر والثقة المعرفية للعملاء ذات دلالة إحصائية عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.

يلخص الجدول رقم: (IV-17) مخرجات برنامج (Smart PLS.4) لنتائج تحليل مسار العلاقة بين بعد تتبع الأثر والثقة المعرفية للعملاء المتوصل إليها من النموذج العام للدراسة كالتالي:

الجدول رقم: (IV-17): نتائج تحليل مسار العلاقة بين بعد تتبع الأثر والثقة المعرفية للعملاء

المتغير المستقل	المتغير الوسيط				
	الثقة المعرفية للعملاء				
تتبع الأثر	معامل المسار	معامل R^2	قيمة T	مستوى P	النتيجة
	0.689	0.225	2.905	0.00	يوجد تأثير

المصدر: من إعداد الطالب بناء على نتائج برنامج (Smart PLS.4)

من خلال الشكل رقم: (IV-11) والجدول رقم: (IV-17) تشير النتائج إلى أن معامل مسار متغير تتبع الأثر على الثقة المعرفة للعملاء قد بلغت قيمته (0.689)، حيث يشر هذا المعامل إلى ارتباط إيجابي قوي بين المتغيرين، في حين أن معامل التحديد R^2 يفيد بأن نسبة 22% من التغير في الثقة المعرفية للعملاء يعود إلى تأثير تتبع الأثر، ونسبة 78% من التغيرات تعود إلى عوامل أخرى، كما تشير النتائج إلى أن القيمة الاحتمالية P بلغت 0.00 وهي أقل من مستوى الدلالة المعتمدة في الدراسة (α=0.05) عند مستوى ثقة 95%، فضلا عن قيمة T المحسوبة التي بلغت (2.905) أكبر من قيمة T الجدولية (1.96)، وهذا يعني وجود أثر ذو دلالة إحصائية.

وبناء على ذلك يتم قبول الفرضية الفرعية الفرعية الخامسة (**H1-5**) التي تنص على أن:

هناك تأثير مباشر بين تتبع الأثر والثقة المعرفية للعملاء عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية

6. اختبار الفرضية الفرعية السادسة:

H1-6 : هناك تأثير مباشر بين سرية البيانات والثقة العاطفية للعملاء عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.

يلخص الجدول رقم: (IV-18) مخرجات برنامج (Smart PLS.4) لنتائج تحليل مسار العلاقة بين بعد سرية البيانات والثقة العاطفية للعملاء المتوصل اليها من النموذج العام للدراسة كالتالي:

الجدول رقم: (IV-18): نتائج تحليل مسار العلاقة بين بعد سرية البيانات والثقة العاطفية للعملاء

المتغير المستقل	المتغير الوسيط				
	الثقة العاطفية للعملاء				
سرية البيانات	معامل المسار	معامل R^2	قيمة T	مستوى P	النتيجة
	0.414	0.222	9.561	0.00	يوجد تأثير

المصدر: من إعداد الطالب بناء على نتائج برنامج (Smart PLS.4)

من خلال الشكل رقم: (IV-11) والجدول رقم: (IV-18) تشير النتائج إلى أن معامل مسار متغير سرية البيانات على الثقة العاطفية للعملاء قد بلغت قيمته (0.414)، حيث يشر هذا المعامل إلى ارتباط إيجابي قوي بين المتغيرين، في حين أن معامل التحديد R^2 يفيد بأن نسبة 22% من التغير في الثقة العاطفية للعملاء يعود إلى تأثير سرية البيانات، ونسبة 78% من التغيرات تعود إلى عوامل أخرى، كما تشير النتائج إلى أن القيمة الاحتمالي P بلغت 0.00 وهي أقل من مستوى الدلالة المعتمدة في الدراسة (α=0.05) عند مستوى ثقة 95%، فضلا عن قيمة T المحسوبة التي بلغت (9.561) أكبر من قيمة T الجدولية (1.96)، وهذا يعني وجود أثر ذو دلالة إحصائية.

وبناء على ذلك يتم قبول الفرضية الفرعية السادسة (**H1-6**) الآتية:

هناك تأثير مباشر بين سرية البيانات والثقة العاطفية للعملاء عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.

7. اختبار الفرضية الفرعية السابعة:

H1-7: هناك تأثير مباشر بين التوافر والديمومة والثقة العاطفية للعملاء عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.

يلخص الجدول رقم: (IV-19) مخرجات برنامج (Smart PLS.4) لنتائج تحليل مسار العلاقة بين بعد التوافر والديمومة والثقة العاطفية للعملاء المتوصل إليها من النموذج العام للدراسة كالتالي:

الجدول رقم (IV-19): نتائج تحليل مسار العلاقة بين بعد التوافر والديمومة والثقة العاطفية للعملاء

المتغير المستقل	المتغير الوسيط				
	الثقة العاطفية للعملاء				
التوافر والديمومة	معامل المسار	معامل R^2	قيمة T	مستوى P	النتيجة
	-0.201	0.194	-1.652	0.109	لا يوجد تأثير

المصدر: من إعداد الطالب بناء على نتائج برنامج (Smart PLS.4)

من خلال الشكل رقم: (IV-11) والجدول رقم: (IV-19) تظهر النتائج بأن معامل مسار متغير التوافر والديمومة على الثقة العاطفية للعملاء قد بلغت قيمته (0.201-)، ويشر هذا المعامل إلى علاقة ارتباط سلبية متوسطة بين المتغيرين، ومن متابعة قيمة T المحسوبة (1.652-) فهي أقل من قيمة T الجدولية (1.96) والقيمة المعنوية P بلغت 0.109 وهي أكبر من مستوى الدلالة المعتمدة في الدراسة (α=0.05) عند مستوى ثقة 95%، وبهذا فالنتائج هي تشير إلى عدم وجود علاقة ارتباطية موجبة بين متغير التوافر والديمومة والثقة العاطفية للعملاء.

وبناء على ذلك يتم **رفض الفرضية الفرعية السابعة (H1-7)** وقبول الفرضية الصفرية التالية:

لا يوجد تأثير مباشر بين التوافر والديمومة والثقة العاطفية للعملاء عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية

08.اختبار الفرضية الفرعية الثامنة:

H1-8: هناك تأثير مباشر بين التكنولوجيا المستخدمة والثقة العاطفية للعملاء عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.

يلخص الجدول رقم: (IV-20) مخرجات برنامج (Smart PLS.4) لنتائج تحليل مسار العلاقة بين بعد التكنولوجيا المستخدمة والثقة العاطفية للعملاء المتوصل إليها من النموذج العام للدراسة كالتالي:

الجدول رقم: (IV-20): نتائج تحليل مسار العلاقة بين بعد التكنولوجيا المستخدمة والثقة العاطفية للعملاء

المتغير المستقل	المتغير الوسيط				
	الثقة العاطفية للعملاء				
التكنولوجيا المستخدمة	معامل المسار	معامل R^2	قيمة T	مستوى P	النتيجة
	0.080	0.301	2.117	0.01	يوجد تأثير

المصدر: من اعداد الطالب بناء على نتائج برنامج (Smart PLS.4)

من خلال الشكل رقم: (IV-11) والجدول رقم: (IV-20) تشير النتائج إلى أن معامل مسار متغير التكنولوجيا المستخدمة على الثقة العاطفية للعملاء قد بلغت قيمته (0.080)، حيث يشر هذا المعامل إلى ارتباط إيجابي ضعيف جدا بين المتغيرين، في حين أن معامل التحديد R^2 يفيد بأن نسبة 30% من التغير في الثقة العاطفية للعملاء يعود إلى تأثير التكنولوجيا المستخدمة، ونسبة 70% من التغيرات تعود إلى عوامل أخرى، كما تشير النتائج إلى أن القيمة الاحتمالي P بلغت 0.00 وهي أقل من مستوى الدلالة المعتمدة في الدراسة (α=0.05) عند مستوى ثقة 95%، فضلا عن قيمة T المحسوبة التي بلغت (2.117) أكبر من قيمة T الجدولية (1.96)، وهذا يعني وجود أثر ذو دلالة إحصائية.

وبناء على ذلك يتم قبول الفرضية الفرعية الثامنة (**H1-8**) التالية:

هناك تأثير مباشر بين التكنولوجيا المستخدمة والثقة العاطفية للعملاء عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.

9.اختبار الفرضية الفرعية التاسعة:

H1-9: هناك تأثير مباشر بين احترام الخصوصية والثقة العاطفية للعملاء ذات دلالة إحصائية عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.

يلخص الجدول رقم: (IV-21) مخرجات برنامج (Smart PLS.4) لنتائج تحليل مسار العلاقة بين بعد احترام الخصوصية والثقة العاطفية للعملاء المتوصل إليها من النموذج العام للدراسة كالتالي:

الجدول رقم (IV-21): نتائج تحليل مسار العلاقة بين بعد احترام الخصوصية والثقة العاطفية للعملاء

المتغير المستقل	المتغير الوسيط				
	الثقة العاطفية للعملاء				
احترام الخصوصية	معامل المسار	معامل R^2	قيمة T	مستوى P	النتيجة
	0.204	0.335	13.919	0.00	يوجد تأثير

المصدر: من إعداد الطالب بناء على نتائج برنامج (Smart PLS.4)

من خلال الشكل رقم: (IV-11) والجدول رقم: (IV-21) تشير النتائج إلى أن معامل مسار متغير احترام الخصوصية على الثقة العاطفية للعملاء قد بلغت قيمته (0.204)، حيث يشر هذا المعامل إلى ارتباط إيجابي متوسط بين المتغيرين، في حين أن معامل التحديد R^2 يفيد بأن نسبة 33% من التغير في الثقة العاطفية للعملاء يعود إلى تأثير احترام الخصوصية، ونسبة 67% من التغيرات تعود إلى عوامل أخرى، كما تشير النتائج إلى أن القيمة الاحتمالي P بلغت 0.00 وهي أقل من مستوى الدلالة المعتمدة في الدراسة (α=0.05) عند مستوى ثقة 95%، فضلا عن قيمة T المحسوبة التي بلغت (13.919) أكبر من قيمة T الجدولية (1.96)، وهذا يعني وجود أثر ذو دلالة إحصائية.

ذلك يتم قبول الفرضية الفرعية التاسعة (**H1-9**) التي تنص على أن:

هناك تأثير مباشر بين احترام الخصوصية والثقة العاطفية للعملاء عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية

10.اختبار الفرضية الفرعية العاشرة:

H1-10: هناك تأثير مباشر بين تتبع الأثر والثقة العاطفية للعملاء عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.

يلخص الجدول رقم: (IV-22) مخرجات برنامج (Smart PLS.4) لنتائج تحليل مسار العلاقة بين بعد تتبع الأثر والثقة العاطفية للعملاء المتوصل إليها من النموذج العام للدراسة كالتالي:

الجدول رقم (IV-22): نتائج تحليل مسار العلاقة بين بعد تتبع الأثر والثقة العاطفية للعملاء

المتغير المستقل	المتغير الوسيط				
	الثقة العاطفية للعملاء				
تتبع الأثر	معامل المسار	معامل R^2	قيمة T	مستوى P	النتيجة
	-0.197	0.311	30.172	0.209	لا يوجد تأثير

المصدر: من اعداد الطالب بناء على نتائج برنامج (Smart PLS.4)

من خلال الشكل رقم: (IV-11) والجدول رقم: (IV-22) تظهر النتائج بأن معامل مسار متغير تتبع الأثر على الثقة العاطفية للعملاء قد بلغت قيمته (0.197-)، ويشر هذا المعامل إلى علاقة ارتباط سلبية متوسطة بين المتغيرين، ومن متابعة قيمة T المحسوبة (30.172) فهي أقل من قيمة T الجدولية (1.96) والقيمة المعنوية P بلغت 0.109 وهي أكبر من مستوى الدلالة المعتمدة في الدراسة (α=0.05) عند مستوى ثقة 95%، وبهذا فالنتائج هي تشير إلى عدم وجود علاقة ارتباطية موجبة بين متغير تتبع الأثر والثقة العاطفية للعملاء.

وبناء على ذلك يتم **رفض الفرضية الفرعية العاشرة (H1-10)** وقبول الفرضية الصفرية التالية:

لا يوجد تأثير مباشر بين تتبع الأثر والثقة العاطفية للعملاء عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية

ثانيا: اختبار وتحليل مسار الفرضية الرئيسية الثانية:

H2: هناك تأثير مباشر ذو دلالة إحصائية عند مستوى دلالة 0،05 بين أبعاد ثقة العملاء في الخدمات الإلكترونية المصرفية لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية؟

وهذه الفرضية جاءت للإجابة على السؤال الثاني:

ما مدى تأثير أبعاد ثقة العملاء في الخدمات الإلكترونية المصرفية عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية؟

ويمكننا الاستعانة بالفرضيات الفرعية التالية:

H2-1: هناك تأثير مباشر بين الثقة المعرفية للعملاء والخدمات الإلكترونية المصرفية عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية ؟

H2-2: هناك تأثير مباشر بين الثقة العاطفية للعملاء والخدمات الإلكترونية المصرفية عند مستوى دلالة0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية ؟

1.1.اختبار الفرضية الفرعية الأولى:

H2-1 : هناك تأثير مباشر بين الثقة المعرفية للعملاء والخدمات الإلكترونية المصرفية عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية ؟

يلخص الجدول رقم: (53) مخرجات برنامج (SMART PLS.4) لنتائج تحليل مسار العلاقة بين بعد الثقة المعرفية للعملاء والخدمات الإلكترونية المصرفية المستنتجة والمتوصل إليها من النموذج العام للدراسة كالتالي:

الجدول رقم: (IV-23): نتائج تحليل مسار العلاقة بين بعد الثقة المعرفية للعملاء والخدمات الإلكترونية المصرفية

المتغير الوسيط	المتغير التابع				
	الخدمات الإلكترونية المصرفية				
الثقة المعرفية للعملاء	معامل المسار	معامل R^2	قيمة T	مستوى P	النتيجة
	0.700	0.662	5.572	0.00	يوجد تأثير

المصدر: من عداد الطالب بناء على نتائج برنامج (Smart PLS.4)

من خلال الشكل رقم: (IV-11) والجدول رقم: (IV-23) تشير النتائج إلى أن معامل مسار متغير الثقة المعرفية للعملاء على الخدمات الإلكترونية المصرفية قد بلغت قيمته (0.700)، حيث يشر هذا المعامل إلى ارتباط إيجابي قوي جدا بين المتغيرين، في حين أن معامل التحديد R^2 يفيد بأن نسبة 66% من التغير في الخدمات الإلكترونية المصرفية يعود إلى تأثير الثقة المعرفية للعملاء، ونسبة 34% من التغيرات تعود إلى عوامل أخرى، كما تشير النتائج إلى أن القيمة الاحتمالي P بلغت 0.00 وهي أقل من مستوى الدلالة المعتمدة في الدراسة (α=0.05) عند مستوى ثقة 95%، فضلا عن قيمة T المحسوبة التي بلغت (5.572) أكبر من قيمة T الجدولية (1.96)، وهذا يعني وجود أثر ذو دلالة إحصائية.

وبناء على ذلك يتم قبول الفرضية الفرعية الأولى (**H2-1**) التي تنص على:

هناك تأثير مباشر بين الثقة المعرفية للعملاء والخدمات الإلكترونية المصرفية عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.

1.2.اختبار الفرضية الفرعية الثانية:

H2-2 : هناك تأثير مباشر بين الثقة العاطفية للعملاء والخدمات الإلكترونية المصرفية عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية ؟

يلخص الجدول رقم: (IV-24) مخرجات برنامج (SMART PLS.4) لنتائج تحليل مسار العلاقة بين بعد الثقة العاطفية للعملاء والخدمات الإلكترونية المصرفية المستنتجة والمتوصل إليها من النموذج العام للدراسة كالتالي:

الجدول رقم: (IV-24): نتائج تحليل مسار العلاقة بين بعد الثقة العاطفية للعملاء والخدمات الإلكترونية المصرفية

المتغير الوسيط	المتغير التابع				
	الخدمات الإلكترونية المصرفية				
الثقة العاطفية للعملاء	معامل المسار	معامل R^2	قيمة T	مستوى P	النتيجة
	0.060	0.202	0.01	1.976	لا يوجد تأثير

المصدر: من عداد الطالب بناء على نتائج برنامج (Smart PLS.4)

من خلال الشكل رقم: (IV-11) والجدول رقم: (IV-24) تشير النتائج إلى أن معامل مسار متغير الثقة العاطفية للعملاء على الخدمات الإلكترونية المصرفية قد بلغت قيمته (0.060)، حيث يشر هذا المعامل إلى ارتباط إيجابي ضعيفة جدا بين المتغيرين، في حين أن معامل التحديد R^2 يفيد بأن نسبة 6% من التغير في الثقة العاطفية للعملاء يعود إلى تأثير الخدمات الإلكترونية المصرفية، ونسبة 94% من التغيرات تعود إلى عوامل أخرى، كما تشير النتائج إلى أن القيمة الاحتمالي P بلغت (1.976) وهي أكبر من مستوى الدلالة المعتمدة في الدراسة (α=0.05) عند مستوى ثقة 95%، فضلا عن قيمة T المحسوبة التي بلغت (0.01) أقل من قيمة T الجدولية (1.96)، وهذا يعني وجود أثر ذو دلالة إحصائية.

وبناء على ذلك يتم **رفض الفرضية الفرعية (H2-2)** التي تنص على:

لا يوجد تأثير مباشر بين الثقة العاطفية للعملاء والخدمات الإلكترونية المصرفية عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.

ثالثا: اختبار وتحليل مسار الفرضية الرئيسية الثالثة:

H3: هناك تأثير مباشر ذات دلالة إحصائية عند مستوى دلالة 0،05 لأبعاد الأمن السيبراني في الخدمات الإلكترونية المصرفية لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية ؟

وهذه الفرضية جاءت للإجابة على السؤال الرئيسي الثالث:

– ما مدى تأثير أبعاد الأمن السيبراني في الخدمات الإلكترونية المصرفية عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية؟

ويمكننا الاستعانة بالفرضيات الفرعية التالية:

- **H3-1: يوجد تأثير مباشر بين سرية البيانات والخدمات الإلكترونية المصرفية عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.**
- **H3-2: يوجد تأثير مباشر بين التوافر والديمومة والخدمات الإلكترونية المصرفية عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.**
- **H3-3: توجد تأثير مباشر بين التكنولوجيا المستخدمة والخدمات الإلكترونية المصرفية عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.**
- **H3-4: توجد تأثير مباشر بين احترام الخصوصية والخدمات الإلكترونية المصرفية عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.**
- **H3-5: توجد تأثير مباشر بين تتبع الأثر والخدمات الإلكترونية المصرفية عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.**

1. اختبار الفرضية الفرعية الأولى:

- **H3-1 : هناك تأثير مباشر بين سرية البيانات والخدمات الإلكترونية المصرفية عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.**

يلخص الجدول رقم: (IV-25) مخرجات برنامج (SMART PLS.4) لنتائج تحليل مسار العلاقة بين بعد سرية البيانات والخدمات الإلكترونية المصرفية المتوصل إليها من النموذج العام للدراسة:

الجدول رقم (IV-25): نتائج تحليل مسار العلاقة بين بعد سرية البيانات والخدمات الإلكترونية المصرفية

المتغير المستقل	المتغير التابع				
	الخدمات الإلكترونية المصرفية				
سرية البيانات	معامل المسار	معامل R^2	قيمة T	مستوى P	النتيجة
	0.689	0.214	5.598	0.00	يوجد تأثير

المصدر: من اعداد الطالب بناء على نتائج برنامج (Smart PLS.4)

من خلال الشكل رقم: (IV-11) والجدول رقم: (IV-25) تشير النتائج إلى أن معامل مسار متغير سرية البيانات على الخدمات الإلكترونية المصرفية قد بلغت قيمته (0.689)، حيث يشر هذا المعامل إلى ارتباط

إيجابي قوي بين المتغيرين، في حين أن معامل التحديد R^2 يفيد بأن نسبة 21% من التغير في الخدمات الإلكترونية المصرفية يعود إلى تأثير سرية البيانات، ونسبة 79% من التغيرات تعود إلى عوامل أخرى، كما تشير النتائج إلى أن القيمة الاحتمالي P بلغت 0.00 وهي أقل من مستوى الدلالة المعتمدة في الدراسة (α=0.05) عند مستوى ثقة 95%، فضلا عن قيمة T المحسوبة التي بلغت (5.598) أكبر من قيمة T الجدولية (1.96)، وهذا يعني وجود أثر ذو دلالة إحصائية.

وبناء على ذلك يتم قبول الفرضية الفرعية الأولى (**H3-1**) التي تنص على:

هناك تأثير مباشر بين سرية البيانات والخدمات الإلكترونية المصرفية عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.

2. اختبار الفرضية الفرعية الثانية:

- **H3-2: هناك تأثير مباشر بين التوافر والديمومة والخدمات الإلكترونية المصرفية عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.**

يلخص الجدول رقم: (IV-26) مخرجات برنامج (SMART PLS.4) لنتائج تحليل مسار العلاقة بين بعد التوافر والديمومة والخدمات الإلكترونية المصرفية المتوصل إليها من النموذج العام للدراسة كالتالي:

الجدول رقم: (IV-26): نتائج تحليل مسار العلاقة بين بعد التوافر والديمومة والخدمات الإلكترونية المصرفية

المتغير المستقل	المتغير التابع				
	الخدمات الإلكترونية المصرفية				
التوافر والديمومة	معامل المسار	معامل R^2	قيمة T	مستوى P	النتيجة
	0.501	0.473	6.490	0.00	يوجد تأثير

المصدر: من اعداد الطالب بناء على نتائج برنامج (Smart PLS.4)

من خلال الشكل رقم: (IV-11) والجدول رقم: (IV-26) تشير النتائج إلى أن معامل مسار متغير التوافر والديمومة على الخدمات الإلكترونية المصرفية قد بلغت قيمته (0.501)، حيث يشر هذا المعامل إلى ارتباط إيجابي قوي بين المتغيرين، في حين أن معامل التحديد R^2 يفيد بأن نسبة 47% من التغير في الخدمات الإلكترونية المصرفية يعود إلى تأثير التوافر والديمومة، ونسبة 53% من التغيرات تعود إلى عوامل أخرى، كما تشير النتائج إلى أن القيمة الاحتمالي P بلغت 0.00 وهي أقل من مستوى الدلالة المعتمدة في الدراسة (α=0.05)

عند مستوى ثقة 95%، فضلا عن قيمة T المحسوبة التي بلغت (6.490) أكبر من قيمة T الجدولية (1.96)، وهذا يعني وجود أثر ذو دلالة إحصائية.

وبناء على ذلك يتم قبول الفرضية الفرعية الثانية (**H3-2**) التي تنص على:

هناك تأثير مباشر بين التوافر والديمومة والخدمات الإلكترونية المصرفية عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.

3. اختبار الفرضية الفرعية الثالثة:

- **H3-3: هناك تأثير مباشر بين التكنولوجيا المستخدمة والخدمات الإلكترونية المصرفية عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.**

يلخص الجدول رقم: (IV-27) مخرجات برنامج (SMART PLS.4) لنتائج تحليل مسار العلاقة بين بعد التكنولوجيا المستخدمة والخدمات الإلكترونية المصرفية المتوصل إليها من النموذج العام للدراسة كالتالي:

الجدول رقم (IV-27): نتائج تحليل مسار العلاقة بين بعد التكنولوجيا المستخدمة والخدمات الإلكترونية المصرفية

المتغير المستقل	المتغير التابع				
	الخدمات الإلكترونية المصرفية				
التكنولوجيا المستخدمة	معامل المسار	معامل R^2	قيمة T	مستوى P	النتيجة
	0.790	0.410	3.972	0.00	يوجد تأثير

المصدر: من اعداد الطالب بناء على نتائج برنامج (Smart PLS.4)

من خلال الشكل رقم: (IV-11) والجدول رقم: (IV-27) تشير النتائج إلى أن معامل مسار متغير التكنولوجيا المستخدمة على الخدمات الإلكترونية المصرفية قد بلغت قيمته (0.790)، حيث يشر هذا المعامل إلى ارتباط إيجابي قوي جدا بين المتغيرين، في حين أن معامل التحديد R^2 يفيد بأن نسبة 41% من التغير في الخدمات الإلكترونية المصرفية يعود إلى تأثير التكنولوجيا المستخدمة، ونسبة 59% من التغيرات تعود إلى عوامل أخرى، كما تشير النتائج إلى أن القيمة الاحتمالي P بلغت 0.00 وهي أقل من مستوى الدلالة المعتمدة في

الدراسة (α=0.05) عند مستوى ثقة 95%، فضلا عن قيمة T المحسوبة التي بلغت (3.972) أكبر من قيمة T الجدولية (1.96)، وهذا يعني وجود أثر ذو دلالة إحصائية.

وبناء على ذلك يتم قبول الفرضية الفرعية الثالثة (**H3-3**)، التي تنص على:

هناك تأثير مباشر بين التكنولوجيا المستخدمة والخدمات الإلكترونية المصرفية عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.

4. اختبار الفرضية الفرعية الرابعة:

- **H3-4: هناك تأثير مباشر بين احترام الخصوصية والخدمات الإلكترونية المصرفية عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.**

يلخص الجدول رقم: (IV-28) مخرجات برنامج (SMART PLS.4) لنتائج تحليل مسار العلاقة بين بعد احترام الخصوصية والخدمات الإلكترونية المصرفية المتوصل إليها من النموذج العام للدراسة كالتالي:

الجدول رقم (IV-28): نتائج تحليل مسار العلاقة بين بعد احترام الخصوصية والخدمات الإلكترونية المصرفية

المتغير المستقل	المتغير التابع				
	الخدمات الإلكترونية المصرفية				
احترام الخصوصية	معامل المسار	معامل R^2	قيمة T	مستوى P	النتيجة
	-1.045	0.123	-1.276	0.304	لا يوجد تأثير

المصدر: من اعداد الطالب بناء على نتائج برنامج (Smart PLS.4)

من خلال الشكل رقم: (47) والجدول رقم: (58) تظهر النتائج بأن معامل مسار احترام الخصوصية على الخدمات الإلكترونية المصرفية قد بلغت قيمته (-1.045)، ويشر هذا المعامل إلى علاقة ارتباط سلبية ضعيفة جدا بين المتغيرين، ومن متابعة قيمة T المحسوبة (-1.276) فهي أقل من قيمة T الجدولية (1.96) والقيمة المعنوية P بلغت (0.304) وهي أكبر من مستوى الدلالة المعتمدة في الدراسة (α=0.05) عند

مستوى ثقة 95%، وبهذا فالنتائج هي تشير إلى عدم وجود علاقة ارتباطية موجبة بين احترام الخصوصية والخدمات الإلكترونية المصرفية.

وبناء على ذلك يتم **رفض الفرضية الفرعية الرابعة (H3-4)** وقبول الفرضية الصفرية التالية:

لا يوجد تأثير مباشر بين احترام الخصوصية والخدمات الإلكترونية المصرفية عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.

5. اختبار الفرضية الفرعية الخامسة:

- **H3-5: هناك تأثير مباشر بين تتبع الأثر والخدمات الإلكترونية المصرفية عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.**

يلخص الجدول رقم: (IV-29) مخرجات برنامج (SMART PLS.4) لنتائج تحليل مسار العلاقة بين بعد تتبع الأثر والخدمات الإلكترونية المصرفية المتوصل إليها من النموذج العام للدراسة كالتالي:

الجدول رقم (IV-29): نتائج تحليل مسار العلاقة بين بعد تتبع الأثر والخدمات الإلكترونية المصرفية

المتغير المستقل	المتغير التابع				
	الخدمات الإلكترونية المصرفية				
تتبع الأثر	معامل المسار	معامل R^2	قيمة T	مستوى P	النتيجة
	0.496	0.180	2.089	0.00	يوجد تأثير

المصدر: من إعداد الطالب بناء على نتائج برنامج (Smart PLS.4)

من خلال الشكل رقم: (IV-11) والجدول رقم: (IV-29) تشير النتائج إلى أن معامل مسار متغير تتبع الأثر على الخدمات الإلكترونية المصرفية قد بلغت قيمته (0.496)، حيث يشر هذا المعامل إلى ارتباط إيجابي قوي بين المتغيرين، في حين أن معامل التحديد R^2 يفيد بأن تتبع الأثر يفسر فقط نسبة 18% من التغير في الخدمات الإلكترونية المصرفية، ونسبة 82% من التغيرات تعود إلى عوامل أخرى، كما تشير النتائج إلى أن القيمة الاحتمالي P بلغت 0.00 وهي أقل من مستوى الدلالة المعتمدة في الدراسة (α=0.05) عند مستوى ثقة 95%، فضلا عن قيمة T المحسوبة التي بلغت (2.089) أكبر من قيمة T الجدولية (1.96)، وهذا يعني وجود أثر ذو دلالة إحصائية.

وبناء على ذلك يتم قبول الفرضية الفرعية الخامسة **(H3-5)** الآتية:

هناك تأثير مباشر بين تتبع الأثر والخدمات الإلكترونية المصرفية عند مستوى دلالة 0،05 لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.

❖ **من هنا بينت تقديرات مؤشرات نموذج الدراسة ما يلي:**

✓ **رفض العلاقة بين التوافر والديمومة والثقة العاطفية للعملاء** ذلك لكون العلاقة غير معنوية:

(p-value=0,109)، وكذا قيمة T المحسوبة (1.652-) فهي أقل من قيمة T الجدولية (1.96).

✓ **رفض العلاقة بين بعد احترام الخصوصية وبعد الثقة المعرفية للعملاء** ذلك لكون العلاقة غير معنوية:

(p-value=0,176)، وكذا قيمة T المحسوبة (0.333) فهي أقل من قيمة T الجدولية (1.96).

✓ **رفض العلاقة بين تتبع الأثر والثقة العاطفية للعملاء** كون العلاقة غير معنوية: (p-value=0,209).

✓ **رفض العلاقة بين احترام الخصوصية والخدمات الإلكترونية المصرفية** ذلك لكون العلاقة غير معنوية:

(p-value=0,304)، وكذا قيمة T المحسوبة (1.276-) فهي أقل من قيمة T الجدولية (1.96).

➢ **عليه، قمنا بحذف العلاقات غير المعنوية لقياس العلاقات غير المباشرة، حسب نتائج الجدول التالي:**

جدول رقم (IV-30): نتائج معامل المسار للعلاقات غير المباشرة بين متغيرات الدراسة

الإحصاءات / المتغيرات	معامل المسار	معامل R^2	الانحراف المعياري Stqndqrd Deviqtion	قيمة (T) Statistics	قيمة المعنوية P Values
سرية البيانات------>البعد المعرفي للثقة------> الخدمات الإلكترونية المصرفية	0.781	0.249	0.01	4.222	0.00
سرية البيانات------>البعد العاطفي للثقة------> الخدمات الإلكترونية المصرفية	0.535	0.124	0.01	24.214	0.00
التوافر والديمومة---->البعد المعرفي للثقة----> الخدمات الإلكترونية المصرفية	0.650	0.423	0.04	12.358	0.00
التوافر والديمومة----->البعد العاطفي للثقة----> الخدمات الإلكترونية المصرفية	-1.211	0.280	0.01	-1.279	0.208
التكنولوجيا المستخدمة-->البعد المعرفي للثقة-> الخدمات الإلكترونية المصرفية	0.724	0.542	0.01	14.101	0.00
التكنولوجيا المستخدمة->البعد العاطفي للثقة---> الخدمات الإلكترونية المصرفية	0.411	0.571	0.02	2.147	0.00
احترام الخصوصية--->البعد المعرفي للثقة----> الخدمات الإلكترونية المصرفية	-0.214	0.142	0.01	-1.002	0.601
احترام الخصوصية --->البعد العاطفي للثقة----> الخدمات الإلكترونية المصرفية	0.302	0.075	0.01	11.199	0.00

تتبع الأثر---------> البعد المعرفي للثقة-------> الخدمات الإلكترونية المصرفية	0.611	0.404	0.01	5.214	0.00
تتبع الأثر---------> البعد العاطفي للثقة--------> الخدمات الإلكترونية المصرفية	-1.098	0.231	0.01	3.206	0.510

المصدر: من اعداد الطالب بناء على مخرجات برنامج Smart PLS.4

يلخص الجدول رقم (IV-30): النتائج الخاصة بالمسارات غير المباشرة لمتغيرات الدراسة والقيم الضرورية لفحص الدلالة الإحصائية، وبناء على ذلك يمكن تفريغ المعطيات في جداول حسب فرضيات الدراسة لتأكيدها أو نفيها.

رابعا: اختبار وتحليل مسار الفرضية الرئيسية الرابعة:

– H4: هناك تأثير غير مباشر ذات دلالة إحصائية عند مستوى دلالة 0،05 للأبعاد الأمن السيبراني في الخدمات الإلكترونية المصرفية من خلال ثقة العملاء لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.

وهذه الفرضية جاءت للإجابة على السؤال الرابع:

– هل هناك تأثير غير مباشر ذات دلالة إحصائية لأبعاد الأمن السيبراني في الخدمات الإلكترونية المصرفية من خلال ثقة العملاء لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية BDL بولاية غرداية؟

ويمكننا الاستعانة بالفرضيات الفرعية التالية:

H4-1: هناك تأثير غير مباشر بين سرية البيانات والخدمات الإلكترونية المصرفية في ظل وجود الثقة المعرفية للعملاء كمتغير وسيطي.

H4-2: هناك تأثير غير مباشر بين التوافر والديمومة والخدمات الإلكترونية المصرفية في ظل وجود الثقة المعرفية للعملاء كمتغير وسيطي.

H4-3: هناك تأثير غير مباشر بين التكنولوجيا المستخدمة والخدمات الإلكترونية المصرفية في ظل وجود الثقة المعرفية للعملاء كمتغير وسيطي.

H4-4: هناك تأثير غير مباشر بين احترام الخصوصية والخدمات الإلكترونية المصرفية في ظل وجود الثقة المعرفية للعملاء كمتغير وسيطي.

H4-5: هناك تأثير غير مباشر بين تتبع الأثر والخدمات الإلكترونية المصرفية في ظل وجود الثقة المعرفية للعملاء كمتغير وسيطي.

H4-6: هناك تأثير غير مباشر بين سرية البيانات والخدمات الإلكترونية المصرفية في ظل وجود الثقة العاطفية للعملاء كمتغير وسيطي.

H4-7: هناك تأثير غير مباشر بين التوافر والديمومة والخدمات الإلكترونية المصرفية في ظل وجود الثقة العاطفية للعملاء كمتغير وسيطي.

H4-8: هناك تأثير غير مباشر بين التكنولوجيا المستخدمة والخدمات الإلكترونية المصرفية في ظل وجود الثقة العاطفية للعملاء كمتغير وسيطي.

H4-9: هناك تأثير غير مباشر بين احترام الخصوصية والخدمات الإلكترونية المصرفية في ظل وجود الثقة العاطفية للعملاء كمتغير وسيطي.

H4-10: هناك تأثير غير مباشر بين تتبع الأثر والخدمات الإلكترونية المصرفية في ظل وجود الثقة العاطفية للعملاء كمتغير وسيطي.

1-اختبار الفرضية الفرعية الأولى:

H4-1: هناك تأثير غير مباشر بين سرية البيانات والخدمات الإلكترونية المصرفية في ظل وجود الثقة المعرفية للعملاء كمتغير وسيطي.

سنقوم بتبيان وحساب العلاقة غير المباشرة بين سرية البيانات والخدمات الإلكترونية المصرفية بوجود الثقة المعرفية للعملاء كمتغير وسيط كالآتي:

الجدول رقم (IV-31): نتائج تحليل المسار للعلاقة غير المباشرة بين سرية البيانات والخدمات الإلكترونية المصرفية بوجود الثقة المعرفية للعملاء

المتغير المستقل	المتغير الوسيط	المتغير التابع				
		الخدمات الإلكترونية المصرفية				
سرية البيانات	الثقة المعرفية للعملاء	معامل المسار	معامل R^2	قيمة T	مستوى P	النتيجة
		0.781	0.249	4.222	0.00	يوجد تأثير

المصدر: من اعداد الطالب بناء على نتائج برنامج (Smart PLS.4)

من خلال نتائج الجداول الحاملة للأرقام: (IV-30) و(IV-31) تشير النتائج إلى أن معامل مسار متغير سرية البيانات على الخدمات الإلكترونية المصرفية بوجود الثقة المعرفية للعملاء كمتغير وسيط قد بلغت قيمته (0.781)، حيث يشر هذا المعامل إلى ارتباط إيجابي قوي جدا بين المتغيرين، في حين أن معامل

التحديد R^2 يفيد بأن نسبة 25% من التغير في الخدمات الإلكترونية المصرفية يعود إلى تأثير سرية البيانات في ظل وجود الثقة المعرفية للعملاء، ونسبة 75% من التغيرات تعود إلى عوامل أخرى، كما تشير النتائج إلى أن القيمة الاحتمالي P بلغت 0.00 وهي أقل من مستوى الدلالة المعتمدة في الدراسة (α=0.05) عند مستوى ثقة 95%، فضلا عن قيمة T المحسوبة التي بلغت (4.222) أكبر من قيمة T الجدولية (1.96)، وهذا يعني وجود أثر ذو دلالة إحصائية.

وبناء على ذلك يتم قبول الفرضية الفرعية الأولى (**H4-1**) التالية:

يوجد تأثير غير مباشر بين سرية البيانات والخدمات الإلكترونية المصرفية في ظل وجود الثقة المعرفية للعملاء كمتغير وسيطي.

2- اختبار الفرضية الفرعية الثانية:

H4-2: هناك تأثير غير مباشر بين التوافر والديمومة والخدمات الإلكترونية المصرفية في ظل وجود الثقة المعرفية للعملاء كمتغير وسيطي.

سنقوم بتبيان وحساب العلاقة غير المباشرة بين التوافر والديمومة والخدمات الإلكترونية المصرفية بوجود الثقة المعرفية للعملاء كمتغير وسيط كالتالي:

الجدول رقم (IV-32): نتائج تحليل المسار للعلاقة غير المباشرة بين التوافر والديمومة والخدمات الإلكترونية المصرفية بوجود الثقة المعرفية للعملاء كمتغير وسيط

المتغير المستقل	المتغير الوسيط	المتغير التابع				
		الخدمات الإلكترونية المصرفية				
التوافر والديمومة	الثقة المعرفية للعملاء	معامل المسار	معامل R^2	قيمة T	مستوى P	النتيجة
		0.650	0.423	12.358	0.00	يوجد تأثير

المصدر: من اعداد الطالب بناء على نتائج برنامج (Smart PLS.4)

من خلال نتائج الجداول الحاملة للأرقام: (IV-30) و(IV-32) تشير النتائج إلى أن معامل مسار متغير التوافر والديمومة على الخدمات الإلكترونية المصرفية بوجود الثقة المعرفية للعملاء كمتغير وسيط قد بلغت قيمته (0.650)، حيث يشر هذا المعامل إلى ارتباط إيجابي قوي بين المتغيرين، في حين أن معامل التحديد R^2 يفيد بأن نسبة 42% من التغير في الخدمات الإلكترونية المصرفية يعود إلى تأثير التوافر والديمومة في ظل وجود الثقة المعرفية للعملاء، ونسبة 58% من التغيرات تعود إلى عوامل أخرى، كما تشير النتائج إلى أن

القيمة الاحتمالي P بلغت 0.00 وهي أقل من مستوى الدلالة المعتمدة في الدراسة (α=0.05) عند مستوى ثقة 95%، فضلا عن قيمة T المحسوبة التي بلغت (12.358) أكبر من قيمة T الجدولية (1.96)، وهذا يعني وجود أثر ذو دلالة إحصائية.

وبناء على ذلك يتم قبول الفرضية الفرعية الثانية (**H4-2**):

لا يوجد تأثير غير مباشر بين التوافر والديمومة والخدمات الإلكترونية المصرفية في ظل وجود الثقة المعرفية للعملاء كمتغير وسيطي.

3- اختبار الفرضية الفرعية الثالثة:

H4-3: هناك تأثير غير مباشر بين التكنولوجيا المستخدمة والخدمات الإلكترونية المصرفية في ظل وجود الثقة المعرفية للعملاء كمتغير وسيطي.

سنقوم بتبيان وحساب العلاقة غير المباشرة بين التكنولوجيا المستخدمة والخدمات الإلكترونية المصرفية بوجود الثقة المعرفية للعملاء كمتغير وسيط:

الجدول رقم (IV-33): نتائج تحليل المسار للعلاقة غير المباشرة بين التكنولوجيا المستخدمة والخدمات الإلكترونية المصرفية بوجود الثقة المعرفية للعملاء كمتغير وسيط

المتغير المستقل	المتغير الوسيط	المتغير التابع				
		الخدمات الإلكترونية المصرفية				
التكنولوجيا المستخدمة	الثقة المعرفية للعملاء	معامل المسار	معامل R^2	قيمة T	مستوى P	النتيجة
		0.724	0.542	14.101	0.00	يوجد تأثير

المصدر: من إعداد الطالب بناء على نتائج برنامج (Smart PLS.4)

من خلال نتائج الجداول الحاملة للأرقام: (IV-30) و(IV-33) تشير النتائج إلى أن معامل مسار متغير التكنولوجيا المستخدمة على الخدمات الإلكترونية المصرفية بوجود الثقة المعرفية للعملاء كمتغير وسيط قد بلغت قيمته (0.724)، حيث يشر هذا المعامل إلى ارتباط إيجابي قوي جدا بين المتغيرين، في حين أن معامل التحديد R^2 يفيد بأن نسبة 54% من التغير في الخدمات الإلكترونية المصرفية يعود إلى تأثير

التكنولوجيا المستخدمة في ظل وجود الثقة المعرفية للعملاء، ونسبة 46% من التغيرات تعود إلى عوامل أخرى، كما تشير النتائج إلى أن القيمة الاحتمالي P بلغت 0.00 وهي أقل من مستوى الدلالة المعتمدة في الدراسة (α=0.05) عند مستوى ثقة 95%، فضلا عن قيمة T المحسوبة التي بلغت (14.101) أكبر من قيمة T الجدولية (1.96)، وهذا يعني وجود أثر ذو دلالة إحصائية.

وبناء على ذلك يتم قبول الفرضية الفرعية الثالثة (**H4-3**) الآتية:

هناك تأثير غير مباشر بين التكنولوجيا المستخدمة والخدمات الإلكترونية المصرفية في ظل وجود الثقة المعرفية للعملاء كمتغير وسيطي.

4- اختبار الفرضية الفرعية الرابعة:

H4-4: هناك تأثير غير مباشر بين احترام الخصوصية والخدمات الإلكترونية المصرفية في ظل وجود الثقة المعرفية للعملاء كمتغير وسيطي.

سنقوم بتبيان وحساب العلاقة غير المباشرة بين الممارسات احترام الخصوصية والخدمات الإلكترونية المصرفية بوجود الثقة المعرفية للعملاء كمتغير وسيط كالتالي:

الجدول رقم (IV-34): نتائج تحليل المسار للعلاقة غير المباشرة بين احترام الخصوصية والخدمات الإلكترونية المصرفية بوجود الثقة المعرفية للعملاء كمتغير وسيط

المتغير المستقل	المتغير الوسيط	المتغير التابع				
		الخدمات الإلكترونية المصرفية				
احترام الخصوصية	الثقة المعرفية للعملاء	معامل المسار	معامل R^2	قيمة T	مستوى P	النتيجة
		-0.214	0.142	-1.002	0.601	لا يوجد تأثير

المصدر: من إعداد الطالب بناء على نتائج برنامج (Smart PLS.4)

من خلال نتائج الجداول الحاملة للأرقام: (IV-30) و(IV-34) وتقديرات النموذج العام الخاصة بالعلاقة بين المتغير احترام الخصوصية والثقة المعرفية للعملاء والتي بينت عدم معنوية العلاقة وبالتالي رفضها، فإنه لا يمكننا أن نتكلم عن علاقة غير مباشرة بين احترام الخصوصية والخدمات الإلكترونية المصرفية في ظل وجود

الثقة المعرفية للعملاء كمتغير وسيط. وبالتالي تم مباشرة **رفض الفرضية البديلة الرابعة (H4-4)** وقبول الفرضية العدمية الآتية:

لا يوجد تأثير غير مباشر بين احترام الخصوصية والخدمات الإلكترونية المصرفية في ظل وجود الثقة المعرفية للعملاء كمتغير وسيطي.

5.اختبار الفرضية الفرعية الخامسة:

H4-5: هناك تأثير غير مباشر بين تتبع الأثر والخدمات الإلكترونية المصرفية في ظل وجود الثقة المعرفية للعملاء كمتغير وسيطي.

سنقوم بتبيان وحساب العلاقة غير المباشرة بين تتبع الأثر والخدمات الإلكترونية المصرفية بوجود الثقة المعرفية للعملاء كمتغير وسيط:

الجدول رقم (IV-35): نتائج تحليل المسار للعلاقة غير المباشرة بين تتبع الأثر والخدمات الإلكترونية المصرفية بوجود الثقة المعرفية للعملاء كمتغير وسيط

المتغير المستقل	المتغير الوسيط	المتغير التابع				
		الخدمات الإلكترونية المصرفية				
تتبع الأثر	الثقة المعرفية للعملاء	معامل المسار	معامل R^2	قيمة T	مستوى P	النتيجة
		0.611	0.404	5.214	0.00	يوجد تأثير

المصدر: من اعداد الطالب بناء على نتائج برنامج (Smart PLS.4)

من خلال نتائج الجداول الحاملة للأرقام: (IV-30) و(IV-35) تشير النتائج إلى أن معامل مسار متغير تتبع الأثر على الخدمات الإلكترونية المصرفية بوجود الثقة المعرفية للعملاء كمتغير وسيط قد بلغت قيمته (0.611)، حيث يشر هذا المعامل إلى ارتباط إيجابي قوي بين المتغيرين، في حين أن معامل التحديد R^2 يشير إلى أن تتبع الأثر يفسر فقط 40% من التغير في الخدمات الإلكترونية المصرفية في ظل وجود الثقة المعرفية للعملاء كمتغير وسيط، ونسبة 60% الباقية من التغيرات تعود إلى عوامل أخرى، كما تشير النتائج إلى أن القيمة الاحتمالي P بلغت 0.00 وهي أقل من مستوى الدلالة المعتمدة في الدراسة (α=0.05) عند

مستوى ثقة 95%، فضلا عن قيمة T المحسوبة التي بلغت (5.214) أكبر من قيمة T الجدولية (1.96)، وهذا يعني وجود أثر ذو دلالة إحصائية.

وبناء على ذلك يتم قبول الفرضية الفرعية الخامسة (**H4-5**) التالية:

يوجد تأثير غير مباشر بين تتبع الأثر والخدمات الإلكترونية المصرفية في ظل وجود الثقة المعرفية للعملاء كمتغير وسيطي.

6-اختبار الفرضية الفرعية السادسة:

H4-6: هناك تأثير غير مباشر بين سرية البيانات والخدمات الإلكترونية المصرفية في ظل وجود الثقة العاطفية للعملاء كمتغير وسيطي.

سنقوم بتبيان وحساب العلاقة غير المباشرة بين سرية البيانات والخدمات الإلكترونية المصرفية بوجود الثقة العاطفية للعملاء كمتغير وسيط كالآتي:

الجدول رقم (IV-36): نتائج تحليل المسار للعلاقة غير المباشرة بين سرية البيانات والخدمات الإلكترونية المصرفية بوجود الثقة العاطفية للعملاء كمتغير وسيط

المتغير المستقل	المتغير الوسيط	المتغير التابع				
		الخدمات الإلكترونية المصرفية				
سرية البيانات	الثقة العاطفية للعملاء	معامل المسار	معامل R^2	قيمة T	مستوى P	النتيجة
		0.535	0.124	24.214	0.00	يوجد تأثير

المصدر: من اعداد الطالب بناء على نتائج برنامج (Smart PLS.4)

من خلال نتائج الجداول الحاملة للأرقام: (IV-30) و(IV-36) تشير النتائج إلى أن معامل مسار متغير سرية البيانات على الخدمات الإلكترونية المصرفية في ظل وجود الثقة العاطفية للعملاء، قد بلغت قيمته (0.535)، حيث يشر هذا المعامل إلى ارتباط إيجابي قوي بين المتغيرين، في حين أن معامل التحديد R^2 يفيد بأن نسبة 12% من التغير في الخدمات الإلكترونية المصرفية يعود إلى تأثير سرية البيانات بوجود الثقة العاطفية للعملاء كمتغير وسيط، ونسبة 88% من التغيرات تعود إلى عوامل أخرى، كما تشير النتائج إلى أن القيمة الاحتمالي P بلغت 0.00 وهي أقل من مستوى الدلالة المعتمدة في الدراسة (α=0.05) عند مستوى

ثقة 95%، فضلا عن قيمة T المحسوبة التي بلغت (24.214) أكبر من قيمة T الجدولية (1.96)، وهذا يعني وجود أثر ذو دلالة إحصائية.

وبناء على ذلك يتم قبول الفرضية الفرعية السادسة (**H4-6**) التالية:

هناك تأثير غير مباشر بين سرية البيانات والخدمات الإلكترونية المصرفية في ظل وجود الثقة العاطفية للعملاء كمتغير وسيطي.

7-اختبار الفرضية الفرعية السابعة:

H4-7: هناك تأثير غير مباشر بين التوافر والديمومة والخدمات الإلكترونية المصرفية في ظل وجود الثقة العاطفية للعملاء كمتغير وسيطي.

سنقوم بتبيان وحساب العلاقة غير المباشرة بين التوافر والديمومة والخدمات الإلكترونية المصرفية بوجود الثقة العاطفية للعملاء كمتغير وسيط كالتالي:

الجدول رقم (IV-37): نتائج تحليل المسار للعلاقة غير المباشرة بين التوافر والديمومة والخدمات الإلكترونية المصرفية بوجود الثقة العاطفية للعملاء كمتغير وسيط

المتغير المستقل	المتغير الوسيط	المتغير التابع				
		الخدمات الإلكترونية المصرفية				
التوافر والديمومة	الثقة العاطفية للعملاء	معامل المسار	معامل R^2	قيمة T	مستوى P	النتيجة
		-1.211	0.280	-1.279	0.208	لا يوجد تأثير

المصدر: من اعداد الطالب بناء على نتائج برنامج (Smart PLS.4)

من خلال نتائج الجداول الحاملة للأرقام: (IV-30) و(IV-37) وتقديرات النموذج العام الخاصة بالعلاقة بين متغير التوافر والديمومة والثقة العاطفية للعملاء التي بينت **عدم معنوية العلاقة** وبالتالي رفضها، فإنه لا يمكننا أن نتكلم عن علاقة غير مباشرة بين التوافر والديمومة والخدمات الإلكترونية المصرفية في ظل وجود الثقة العاطفية للعملاء كمتغير وسيط. وعليه تم مباشرة **رفض الفرضية البديلة السابعة** (**H4-7**) وقبول الفرضية العدمية:

لا يوجد تأثير غير مباشر بين التوافر والديمومة والخدمات الإلكترونية المصرفية في ظل وجود الثقة العاطفية للعملاء كمتغير وسيطي.

8-اختبار الفرضية الفرعية الثامنة:

H4-8: هناك تأثير غير مباشر بين التكنولوجيا المستخدمة والخدمات الإلكترونية المصرفية في ظل وجود الثقة العاطفية للعملاء كمتغير وسيطي.

سنقوم بتبيان وحساب العلاقة غير المباشرة بين التكنولوجيا المستخدمة والخدمات الإلكترونية المصرفية بوجود الثقة العاطفية للعملاء كمتغير وسيط:

الجدول رقم (IV-38): نتائج تحليل المسار للعلاقة غير المباشرة بين التكنولوجيا المستخدمة والخدمات الإلكترونية المصرفية بوجود الثقة العاطفية للعملاء كمتغير وسيط

المتغير المستقل	المتغير الوسيط	المتغير التابع				
		الخدمات الإلكترونية المصرفية				
التكنولوجيا المستخدمة	الثقة العاطفية للعملاء	معامل المسار	معامل R^2	قيمة T	مستوى P	النتيجة
		0.214	0.571	2.147	0.00	يوجد تأثير

المصدر: من إعداد الطالب بناء على نتائج برنامج (Smart PLS.4)

من خلال نتائج الجداول الحاملة للأرقام: (IV-30) و(IV-38) تشير النتائج إلى أن معامل مسار متغير التكنولوجيا المستخدمة على الخدمات الإلكترونية المصرفية في ظل وجود الثقة العاطفية للعملاء كمتغير وسيط قد بلغت قيمته (0.214)، حيث يشر هذا المعامل إلى ارتباط إيجابي متوسط بين المتغيرين، في حين أن معامل التحديد R^2 يفيد بأن نسبة 57% من التغير في الثقة المعرفية للعملاء يعود إلى تأثير سرية البيانات، ونسبة 43% من التغيرات تعود إلى عوامل أخرى، كما تشير النتائج إلى أن القيمة الاحتمالي P بلغت 0.00 وهي أقل من مستوى الدلالة المعتمدة في الدراسة (α=0.05) عند مستوى ثقة 95%، فضلا عن قيمة T المحسوبة التي بلغت (2.147) أكبر من قيمة T الجدولية (1.96)، وهذا يعني وجود أثر ذو دلالة إحصائية.

وبناء على ذلك يتم قبول الفرضية الفرعية الثامنة (**H4-8**) التالية:

هناك تأثير غير مباشر بين التكنولوجيا المستخدمة والخدمات الإلكترونية المصرفية في ظل وجود الثقة العاطفية للعملاء كمتغير وسيطي.

9-اختبار الفرضية الفرعية التاسعة:

H4-9: هناك تأثير غير مباشر بين احترام الخصوصية والخدمات الإلكترونية المصرفية في ظل وجود الثقة العاطفية للعملاء كمتغير وسيطي.

سنقوم بتبيان وحساب العلاقة غير المباشرة بين احترام الخصوصية والخدمات الإلكترونية المصرفية بوجود الثقة العاطفية للعملاء كمتغير وسيط كالتالي:

الجدول رقم (IV-39): نتائج تحليل المسار للعلاقة غير المباشرة بين احترام الخصوصية والخدمات الإلكترونية المصرفية بوجود الثقة العاطفية للعملاء كمتغير وسيط

المتغير المستقل	المتغير الوسيط	المتغير التابع				
		الخدمات الإلكترونية المصرفية				
احترام الخصوصية	الثقة العاطفية للعملاء	معامل المسار	معامل R^2	قيمة T	مستوى P	النتيجة
		0.302	0.075	11.199	0.00	يوجد تأثير

المصدر: من إعداد الطالب بناء على نتائج برنامج (Smart PLS.4)

من خلال نتائج الجداول الحاملة للأرقام: (IV-30) و(IV-39) تشير النتائج إلى أن معامل مسار متغير احترام الخصوصية على الخدمات الإلكترونية المصرفية بوجود الثقة العاطفية للعملاء كمتغير وسيط قد بلغت قيمته (0.302)، حيث يشر هذا المعامل إلى ارتباط إيجابي متوسط بين المتغيرين، في حين أن معامل التحديد R^2 يفيد بأن نسبة 07% من التغير في الثقة المعرفية للعملاء يعود إلى تأثير سرية البيانات، ونسبة 93% من التغيرات تعود إلى عوامل أخرى، كما تشير النتائج إلى أن القيمة الاحتمالي P بلغت 0.00 وهي أقل من مستوى الدلالة المعتمدة في الدراسة (α=0.05) عند مستوى ثقة 95%، فضلا عن قيمة T المحسوبة التي بلغت (11.199) أكبر من قيمة T الجدولية (1.96)، وهذا يعني وجود أثر ذو دلالة إحصائية.

وبناء على ذلك يتم قبول الفرضية الفرعية التاسعة (**H4-9**) التالية:

لا يوجد تأثير غير مباشر بين احترام الخصوصية والخدمات الإلكترونية المصرفية في ظل وجود الثقة العاطفية للعملاء كمتغير وسيطي.

10-اختبار الفرضية الفرعية العاشرة:

H4-10: هناك تأثير غير مباشر بين تتبع الأثر والخدمات الإلكترونية المصرفية في ظل وجود الثقة العاطفية للعملاء كمتغير وسيطي.

سنقوم بتبيان وحساب العلاقة غير المباشرة بين تتبع الأثر والخدمات الإلكترونية المصرفية بوجود الثقة العاطفية للعملاء كمتغير وسيط:

الجدول رقم (IV-40): نتائج تحليل المسار للعلاقة غير المباشرة بين تتبع الأثر والخدمات الإلكترونية المصرفية بوجود الثقة العاطفية للعملاء كمتغير وسيط

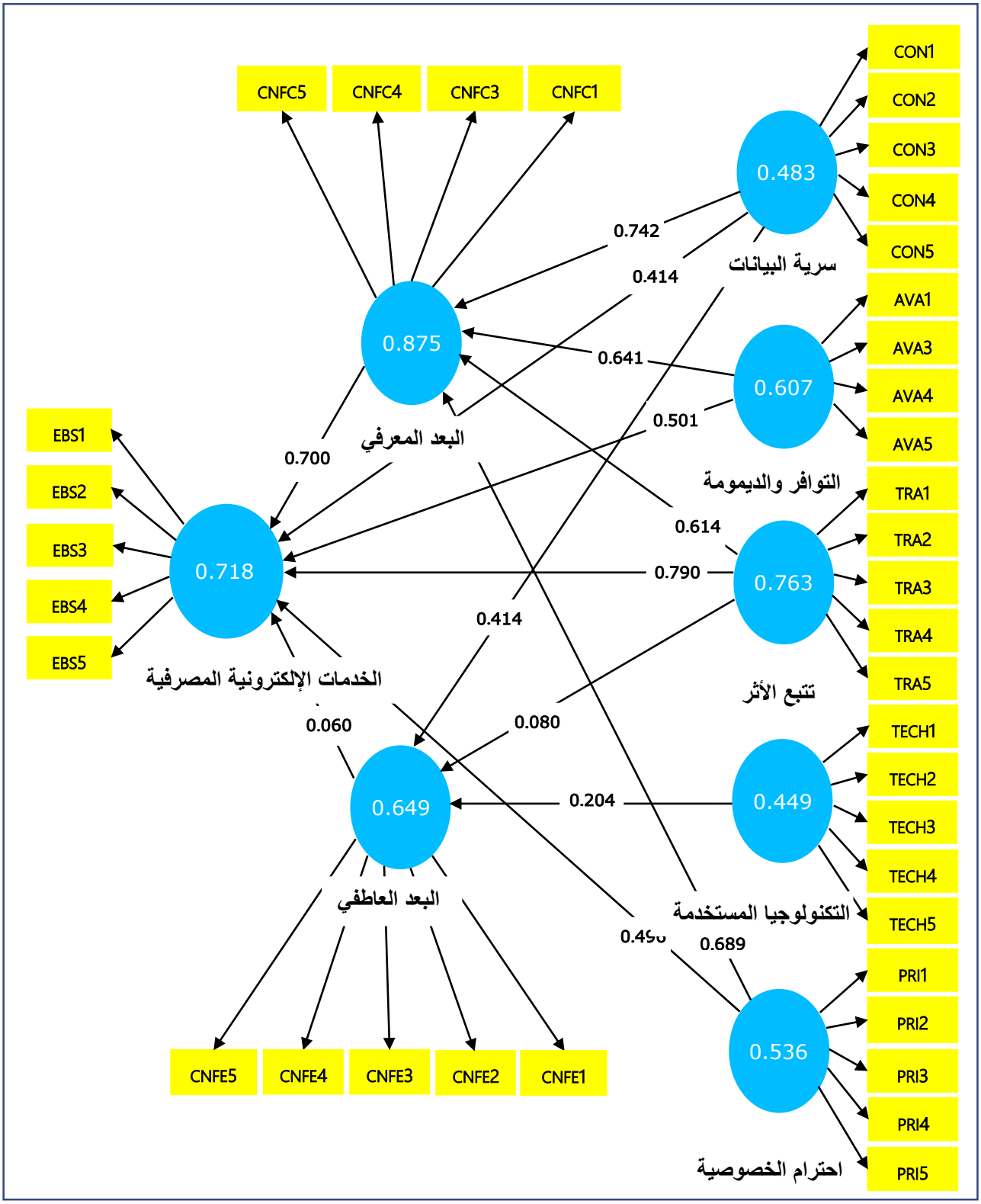
المتغير المستقل	المتغير الوسيط	المتغير التابع				
		الخدمات الإلكترونية المصرفية				
تتبع الأثر	الثقة العاطفية للعملاء	معامل المسار	معامل R^2	قيمة T	مستوى P	النتيجة
		-1.098	0.291	3.206	0.00	لا يوجد تأثير

المصدر: من اعداد الطالب بناء على نتائج برنامج (Smart PLS.4)

من خلال نتائج الجداول الحاملة للأرقام: (IV-30) و(IV-40) وتقديرات النموذج العام الخاصة بالعلاقة بين المتغير تتبع الأثر والثقة العاطفية للعملاء التي بينت **عدم معنوية العلاقة** وبالتالي رفضها، فإنه لا يمكننا أن نتكلم عن علاقة غير مباشرة بين تتبع الأثر والخدمات الإلكترونية المصرفية في ظل وجود الثقة العاطفية للعملاء كمتغير وسيط. وبالتالي تم مباشرة **رفض الفرضية البديلة العاشرة (H4-10)** وقبول الفرضية العدمية:

لا يوجد تأثير غير مباشر بين تتبع الأثر والخدمات الإلكترونية المصرفية في ظل وجود الثقة العاطفية للعملاء كمتغير وسيطي.

الشكل رقم (IV-12): النموذج النهائي المعدل المقترح للدراسة



المصدر: من اعداد الطالب بناء على نتائج برنامج (Smart PLS.4)

➢ ملاحظة: تم التأكد من معنوية العلاقات غير المباشرة عن طريق البوتسراب (Bootstrapping).

المطلب الثالث: تفسير ومناقشة النتائج

على ضوء نتائج الدراسة، في هذا المطلب سيتم عرضها لمناقشتها وتفسيرها كما يلي:

1-حسب إجابات الأفراد حول متغيرات الدراسة:

1.1-الأمن السيبراني: يعتبر مصطلح الأمن السيبراني واحدا من المصطلحات الحديثة في عصرنا الحالي، تطور بتطور تقنية الاعلام والاتصال وتوسع استعمال شبكة الإنترنت في شتى المجالات خاصة منها التجارية وما تعلق منها بالمعاملات المالية المصرفية، فالأمن السيبراني بمجموعة مكوناته وأبعاده المتعلقة بالوسائل التقنية والإدارية التي يتم القيام بها لمنع الاستخدام غير المشروع، وكذا سوء استغلال المعلومات الإلكترونية ونظم الاتصالات والبيانات التي تحتويها، هدفه ضمان توافر واستمرارية عمل النُظم، وكذا تأمين حماية سرية وخصوصية البيانات الشخصية، وحماية المستخدمين من المخاطر في الفضاء السيبراني أي توفر الأبعاد الخمسة المتمثلة في: (سرية البيانات، التوافر والديمومة، التكنولوجيا المستخدمة، احترام الخصوصية، تتبع الأثر)، وفق هذه الرؤية تشير اتجاهات وآراء أفراد العينة المستجوبة في الدراسة الحالية لعملاء بنك التنمية المحلية غرداية أن الأمن السيبراني للبنك محل الدراسة كان ضمن درجة موافقة مقبولة، ويرجع ذلك إلى تقييم موضوعي مبني على أساس أن إجراءات الأمن السيبراني للمعاملات المالية بالبنك سليمة تخضع للشركة الجزائرية لأتمته المعاملات بين البنوك المسماة Société Algérienne d'automatisations des Transaction (SATIM) وكذا لرقابة أجهزة الدولة.

بالنسبة للمعدل العام للمتوسطات الحسابية لكل أبعاد الأمن السيبراني (سرية البيانات، التوافر والديمومة، التكنولوجيا المستخدمة، احترام الخصوصية، تتبع الأثر)، فقد كان ضمن مجال الموافقة المتوسط بقيمة 4.05، تقابله نسبة 81%، التي تعكس نسبة ممتازة ومقبولة في اجتماع الآراء على أن بنك التنمية المحلية غرداية يتمتع بأمن سيبراني جد ومقبول إلى حد بعيد.

2.1-ثقة العملاء: إن اتجاهات أفراد العينة نحو أبعاد الثقة (البعد المعرفي والبعد العاطفية) شهدت مستوى مرتفع في درجة التقييم ويعزى ذلك إلى جوانب الأمان المتعلقة باستخدام الخدمات الإلكترونية المصرفية من إجراءات وتدابير أمنية، وكذا قدرة وكفاءة بنك التنمية المحلية في تقديم خدماته إلكترونيا مع استجابته السريعة لحل أي مشكل يتعلق بسلامة وأمن المعاملات الإلكترونية، ضف إلى ذلك شعور العملاء بالأمان في التعامل وحماية بياناتهم الشخصية تبعا للقوانين والسياسة الموجودة.

أما بالنسبة للمعدل العام للمتوسطات الحسابية لبعد ثقة العملاء، يلخص التقييم العام لهم اتجاه الخدمات الإلكترونية المصرفية التي يقدمها بنك التنمية المحلية وأمنه السيبراني فقد كان ضمن مجال الموافقة المتوسط

بقيمة 3.85، تقابله النسبة المؤوية 77%، التي تعكس نسبة جيدة ومقبولة، وهذا يعني أن عملاء بنك التنمية المحلية يشعرون بمستوى مرتفع من الثقة فيما يتعلق بأمن الخدمات الإلكترونية المصرفية التي تقدم لهم.

3.1-الخدمات الإلكترونية المصرفية: الملاحظ أن آراء واتجاهات أفراد العينة المستجوبة المتعلقة بمتغير الخدمات الإلكترونية المصرفية المقدمة لهم من قبل بنك التنمية المحلية بغرداية، ضمن مجال الموافقة بمتوسط حسابي إجمال بلغ 3.95 حسب مقياس ليكارت، تقابله نسبة مؤوية 79%، التي تعكس نسبة جيدة ومقبولة، مما يدل على أن عملاء البنك محل الدراسة راضين بمستوى الخدمات الإلكترونية المصرفية المقدمة لهم لتلبية حاجياتهم ورغباتهم باعتبارها الأفضل مقارنة بتلك الخدمات المصرفية التقليدية.

2-اختبار الفرضيات:

يلاحظ من نتيجة اختبار **الفرضية الرئيسية الأولى** تأكيد وجود تأثير مباشر لأبعاد الأمن السيبراني في ثقة العملاء لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية، وبعد الاستعانة بالفرضيات الفرعية لها تحصلنا على ما يلي:

-وفقا لنتائج اختبار الفرضيات الفرعية (الأولى والثانية والثالثة والخامسة) التي تؤكد وجود تأثير مباشر لكل من الأبعاد التالية: (سرية البيانات-التوافر والديمومة-استخدام التكنولوجيا-تتبع الأثر) في الثقة المعرفية لعملاء بنك التنمية المحلية، كون أكثر ما يهم عملاء اليوم في معاملاتهم المالية الإلكترونية مع البنك هو سرية بياناتهم الشخصية وعدم تركها عرضة للاطلاع، فاستغلال البنك لهذا البعد من خلال عملية تثقيف العميل وإثراء معارفه بخصوص كيفية التعامل مع تركيبة الأرقام السرية وطرق تجنب قرصنتها بداية من يوم تسليمه بطاقة الدفع الإلكترونية، وكذا توعيته بإجراءات عملية التشفير سواء بالبصمة الرقمية أو التوقيع الإلكتروني، فذلك يزيد في الثقة المعرفية للعميل، كذا هو الحال بالنسبة لبعد التوافر والديمومة، فضمان بنك التنمية المحلية لقابلية الوصول للخدمة حين الطلب عليها واتاحتها 24/24 سا تزيد من الثقة المعرفية للعملاء واعتقادهم بكفاءة البنك وخبرته لتأمين خدمة التعامل معه إلكترونيا، ضف إلى ذلك حداثة التكنولوجيا المستخدمة من قبل البنك بتوفيره الأجهزة والبرامج والأنظمة والشبكات والبنية التحتية الرقمية، أما ما تعلق بالدليل المادي بوجود خدمة من خلالها تضمن عدم إنكار أي شخص أو جهة قامت بتصرف ما متصل بالبيانات وتتبع أثره، وتسجيل جميع المعاملات آليا في الفضاء الإلكتروني، أثر ذلك كله بشكل مباشرة على الثقة المعرفية للعميل.

أما بالنسبة للفرضية الفرعية (الرابعة) التي بينت نتائجها بعدم وجود تأثير مباشر لبعد احترام الخصوصية في الثقة المعرفية للعملاء، يمكننا تفسير ذلك أن البنك محل الدراسة لم يقدم أي إجراءات عملية تُحسس العميل بضمان احترام خصوصيته، خاصة وأن مقدمو الخدمات بالبنك يطلبون من العملاء الإدلاء ببعض المعلومات التي لا يقبلون الإفصاح عنها مثلا: مقر الإقامة بالضبط، رقم الهاتف بالنسبة للإناث، رأس المال المملوك، مختلف المشاريع المالية...إلخ.

-الفرضيات الفرعية (السادسة والثامنة والتاسعة) أكدت على وجود تأثير مباشر لكل من الأبعاد التالية: (سرية البيانات-استخدام التكنولوجيا-احترام الخصوصية) في الثقة العاطفية للعملاء، كون البعد العاطفي يتعلق أساسا بمستوى الصدق والأمانة والالتزام ودرجة الإحسان للشريك (البنك ممثلا بموظفيه ومقدمو خدماته) والتي وضعها العملاء فيهم وهذا ما لاحظناه في دراستنا من خلال النتائج، وهي جد مهمة في بعد الثقة، فكل من الأبعاد السالفة الذكر لها تغذية عكسية على مستوى الصدق والأمانة، وحتما هذا ما يحقق رضا العملاء ويولد الاستمرارية في التعامل.

أما بالنسبة لنتائج الفرضيات الفرعية (السابعة والعاشرة) أظهرت عدم وجود تأثير مباشر بين كل من بعد (التوافر والديمومة وبعد تتبع الأثر) في الثقة العاطفية للعملاء، ويمكن تفسير ذلك بكون بعد التوافر والديمومة هو مرتبط أساسا بدرجة تدفق الإنترنت، وكما هو معروف أن مستوى تدفقها بالجزائر هو بدرجة غير عالية خاصة في المناطق التي لا تتوفر على التغطية، وهذا ما جعل الثقة العاطفية لعملاء بنك التنمية بغرداية لا تتأثر بشكل مرتفع مع هذا البعد، أما بالنسبة لانعدام التأثير بين بعد تتبع الأثر والثقة العاطفية للعملاء، فالعينة المستجوبة لم تتجاوب مع عبارات هذا البعد بمتوسط موافقة مقبول وكانت العلاقة سلبية، حيث يمكن تفسير ذلك أن العميل يفكر أنه بمجرد وقوعه ضحية أي جريمة إلكترونية فلا فائدة من تتبع الأثر، خاصة وأن العميل الجزائري بصفة عامة والغرداوي بصفة خاصة، هو لا يرغب تماما في دخوله المحاكم والمجالس لأجل المتابعات القضائية.

-بخصوص تفسير إثبات صحة **الفرضية الرئيسية الثانية** بتأكيد وجود تأثير مباشر لأبعاد ثقة العملاء في الخدمات الإلكترونية المصرفية لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية، أنه بعد الاستعانة بالفرضيات الفرعية لها تأكد لنا بوجود تأثير إيجابي مباشر لكل من بعد الثقة المعرفية وبعد الثقة العاطفية للعملاء على الخدمات الإلكترونية المصرفية، كون هاته الأخيرة هي مرتبطة ارتباطا وثيقا بعامل الثقة وشعور العميل بالأمان، فنتائج دراستنا أثبتت أن عملاء البنك محل الدراسة يضعون ثقتهم فيه، ويرجع ذلك إلى السياسة والاستراتيجية الجيدة التي يتبعها في تعامله رقميا ببطاقات دفع وسحب وتحويل عالمية مثل: فيزا كرد وماستر كارد وبطاقة الكوربورايت وأجهزة متطورة وحديثة مثل الموزع الآلي للأوراق Distributeur (DAB) Automatique de Billet، والشباك الآلي البنكي Guichet Automatique de (GAB) Bancairek، ونهائي الدفع الإلكتروني Terminal de Paiement Electronique (TPE) ونظام مالي عالمي للتسوية الإجمالية الفورية Real Time Gross Settlement system (RTGS) بمواصفة قياسية دولية حائزة على الإيزو (ISO).

-**الفرضية الرئيسية الثالثة** أكدت عن وجود تأثير مباشر لأبعاد الأمن السيبراني في الخدمات الإلكترونية المصرفية لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية، فبعد الاستعانة بالفرضيات الفرعية (الأولى والثانية والثالثة والخامسة) لها تأكد لنا وجود تأثير إيجابي مباشر لكل من بعد (سرية البيانات-

التوافر والديمومة–التكنولوجيا المستخدمة–تتبع الأثر) في الخدمات الإلكترونية المصرفية للبنك محل الدراسة، كون جميع هاته الأبعاد هي حجر الأساس لمختلف المعاملات الرقمية، فدونها لا يمكن الحديث عن تقديم خدمات بأرياحية للعميل، سواء من حيث أمنها وسلامتها أو من حيث توافرها وتوزيعها، ومن الجهة المقابلة فالعملاء لا يقدمون إطلاقا في التعامل رقميا مع أي مؤسسة كانت بنيتها الرقمية هشة أو نوعية أجهزتها ونظمها وشبكات اتصالها غير متطورة بما يعرض أموالها للخطر أو الضرر، فالعميل لا يخاطر إطلاقا في هذا المجال.

أما بالنسبة للفرضية الفرعية (الرابعة) التي بينت نتائجها بعدم وجود تأثير مباشر لبعد احترام الخصوصية في الخدمات الإلكترونية المصرفية، أنه يمكن تفسير ذلك أن البنك حين تقديمه للعملاء مجموعة متنوعة من الخدمات الإلكترونية المصرفية فهو لا يقدر أن يضمن احترام خصوصية جميع شرائح المجتمع، كون رضا الناس غاية لا تدرك، مثلا: ما هو حلال عند البعض هو حرام عند الآخر، وما يراه طرف معينة أنه خصوصي يراه الآخر أنه غير ذلك، فمستوى الثقافة والتعلم والوعي والتقاليد والخصوصية هي تختلف من عميل لآخر.

–أما بخصوص تفسير إثبات صحة **الفرضية الرئيسية الرابعة** بوجود تأثير غير مباشر لأبعاد الأمن السيبراني في الخدمات الإلكترونية المصرفية من خلال وجود ثقة العملاء كمتغير وسيط لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية، أنه بعد الاستعانة بالفرضيات الفرعية لها تحصلنا على:

–تبعا لنتائج اختبار الفرضيات الفرعية (الأولى والثانية والثالثة والخامسة) التي تؤكد وجود تأثير غير مباشر لكل من الأبعاد التالية: (سرية البيانات–التوافر والديمومة–التكنولوجيا المستخدمة–تتبع الأثر) في الخدمات الإلكترونية المصرفية من خلال وجود الثقة المعرفية للعملاء كمتغير وسيط، حيث تتوافق هذه النتيجة مع ما سبق ذكره في الفرضية الرئيسية الأولى والثانية والثالثة، كون نفس أبعاد الأمن السيبراني التي لها تأثير مباشر على الخدمات الإلكترونية المصرفية وكذا لها تأثير مباشر على الثقة المعرفية للعملاء، هي نفسها التي لها تأثير غير مباشر على الخدمات الإلكترونية المصرفية في ظل وجود الثقة المعرفية للعملاء، بل وأن النتائج أظهرت ارتفاع درجة التأثير في العلاقة غير المباشرة بين هذه المتغيرات، نفسر ذلك أن بنك التنمية المحلية من خلال حرصه على توفر عناصر الأمن السيبراني المذكورة أعلاه في عملية إنتاج الخدمات الإلكترونية المصرفية وتقديمها للعملاء بوسائل وتقنيات عالية المستوى أدى هذا إلى رفع من مستوى ثقتهم بها فكانت النتيجة حتما إقبالهم عليها واستخدامهم لها، وكذا هو الحال بالنسبة للبعد الثاني (الثقة العاطفية للعملاء) كمتغير وسيط بين أبعاد الأمن السيبراني والخدمات الإلكترونية المصرفية.

أما فيما يخص نتائج اختبار الفرضية الفرعية (والرابعة) كشفت عن عدم وجود تأثير غير مباشر بين بعد احترام الخصوصية والخدمات الإلكترونية المصرفية في ظل وجود الثقة المعرفية للعملاء، فنفسر هذا أنه لا يمكن الحديث عن علاقة غير مباشرة في ظل عدم معنوية العلاقة المباشرة، ومن نفس المنطلق وبنفس الطريقة نفسر العلاقات المتبقية.

خلاصة الفصل الرابع:

من خلال هذا الفصل، تم استعراض نتائج الدراسة الميدانية، بعد أن كللت عملية توزيع الاستبانة ببلوغ 195 مفردة صالحة للتحليل، وبالاستعانة بالبرنامج التحليل الاحصائي للعلوم الاجتماعية (SPSS V26) تم عرض عدد من الأشكال البيانية والجداول مع دعمها بالشرح والتعليق وتوصيف عام لخصائص العينة المستجوبة، وبعد اختبار مدى اعتدالية توزيع البيانات تقرر الاستعانة أسلوب نمذجة المعادلة الهيكلية (SEM) Structure Equation Modeling بطريقة المربعات الصغرى الجزئية (PLS) Partial Least Squares Path Modeling وذلك من أجل الحصول نتائج أكثر دقة، ولهذا الغرض تم الاعتماد أيضا على البرنامج الاحصائي المتقدم (Smart PLS 4)، عليه تحصلنا على ما يلي:

- درجة مرضية من الصدق والثبات لنموذج القياس.
- جودة وكفاءة نموذج الدراسة الهيكلي الذي يفسر مسار العلاقات بين المتغيرات.
- تم التأكد من عدم وجود التداخل الخطي بين المباني (VIF).
- ملائمة معاملات المسار (Path Coefficients).
- التأكد من قيم كل من معامل التفسير (R^2) وحجم الأثر (F^2).
- نتائج ذات مستوى جد مرضي يمكن الاعتماد عليها للاستمرار في تحليل البيانات واختبار الفرضيات.

في النهاية تم المضي في التحليل والاجابة على تساؤلات الدراسة مع تفسير ومناقشة النتائج، حيث تم إثبات صحة الفرضيات الرئيسية الأربعة المطروحة في البداية المتمثلة في:

- ❖ هناك تأثير مباشر لأبعاد الأمن السيبراني للبيانات في تعزيز ثقة العملاء لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.
- ❖ هناك تأثير مباشر لثقة العملاء في الخدمات الإلكترونية المصرفية لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.
- ❖ هناك تأثير مباشر لأبعاد الأمن السيبراني للبيانات في الخدمات الإلكترونية المصرفية لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.
- ❖ هناك تأثير غير مباشر لأبعاد الأمن السيبراني للبيانات في الخدمات الإلكترونية المصرفية من خلال تعزيز ثقة العملاء لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية.

في الختام، سيقدم الطالب مجموعة من المقترحات لبنك التنمية المحلية لولاية غرداية، يمكن الاستفادة منها لتطوير جانب تقديم الخدمات الإلكترونية المصرفية، وكذا مقترحات تتعلق بتدابير وإجراءات تحسين مستوى أبعاد الأمن السيبراني بهدف تعزيز ثقة العملاء واستمراريتهم في التعامل مع البنك محل الدراسة.

خاتمة

بعد التطرق بإسهاب لمتغيرات الدراسة في فصلها الأول والثاني من أجل وضع إطار نظري لأهم المفاهيم المرتبطة بالأمن السيبراني للبيانات وثقة العملاء والخدمات الإلكترونية المصرفية، ركزت الدراسة في جانبها الميداني على تسليط الضوء على مدى مساهمة أبعاد الأمن السيبراني في تعزيز ثقة العملاء نحو الخدمات الإلكترونية المصرفية، حيث وبعد البرهنة على صحة الفرضيات الموضوعة سابقا باستعمال الاستبيان كأداة رئيسية للدراسة الميدانية وتحليل نتائجه تم التوصل لمجموعة من النتائج في جزئيها النظري والتطبيقي سنستعرض أهمها في النقاط التالية:

نتائج الدراسة:

يمكن عرض الاستنتاجات الخاصة بالجانب النظري والنتائج المتوصل إليها من خلال الدراسة الميدانية كما يلي:

- **استنتاجات الدراسة النظرية:**

– مسألة تحقيق الأمن السيبراني هي جزأ لا يتجزأ من الأمن الوطني والأمن القومي كونه الركن الأساسي وقاعدة نجاح مخططات التنمية والتطوير المجتمعي على شتى الأصعدة وفي مختلف الميادين.

– الأمن السيبراني مسؤولية جميع الأطراف، مما يقتضي التعاون الدولي والمؤسساتي لحمايته.

– الأمن السيبراني هو الحقل الذي يدرُس طرق حماية البيانات المخزنة في أجهزة الحاسوب ومختلف الأجهزة الملحقة وشبكات الاتصالات، وشتى المكينات الرقمية الأخرى بما فيها وسائل الدفع المصرفية الإلكترونية، هدفه التصدي للمحاولات الرامية إلى الدخول غير المشروع إلى قواعد البيانات المخزنة أو تلك التي ترمي إلى التجسس عليها ونقلها أو تغييرها وتخريبها.

– تخلف الجرائم السيبرانية آثارا اقتصادية واجتماعية كارثية.

– الثقة الرقمية هي عامل جد مهم لنجاح المصارف التي تقدم خدمات إلكترونية فهي تعزز قدرتها على تأدية رسالتها ورؤيتها.

– الخدمات الإلكترونية المصرفية أصبحت تمثل الركيزة الأساسية للصناعة المصرفية والعنوان الرئيسي للتعاملات المستقبلية لتلبية حاجات ورغبات العملاء.

- **نتائج الدراسة الميدانية:**

بعد تحليل البيانات التي تم جمعها بالاستبيان ومناقشتها بشكل تفصيلي، يمكن عرض نتائج الدراسة الميدانية كما يلي:

❖ **إثبات ونفي صحة الفرضيات:**

من خلال مسار الدراسة تم التأكد من صحة الفرضيات المطروحة في البداية والتي جاءت كما يلي:

- **الفرضة الرئيسية الأولى:** بعد اختبار الفرضيات الفرعية لها، جاءت جلها تؤكد "**صحة الفرضية الرئيسية الأولى**" وتشير إلى وجود تأثير مباشر لأبعاد الأمن السيبراني (سرية البيانات، التوافر والديمومة، التكنولوجيا المستخدمة، احترام الخصوصية، تتبع الأثر) في ثقة العملاء لدى عينة مستخدمي بطاقات الدفع الإلكترونية ببنك التنمية المحلية بولاية غرداية، حيث تمتع بعدي (سرية البيانات والتكنولوجيا المستخدمة) بأعلى مستوى من التأثير في العلاقة بقيمة بلغت: (0.742 و0.614) على التوالي، ما عدا بعد (احترام الخصوصية) كان تأثيره سلبي بقيمة بلغت: (0.114-).
- **الفرضة الرئيسية الثانية:** بعد الاستعانة بالفرضيات الفرعية لها، تبين لنا وجود تأثير مباشر لثقة العملاء من خلال بعديها (الثقة المعرفية، الثقة العاطفية) في الخدمات الإلكترونية المصرفية، حيث كانت علاقة التأثير قوية بالنسبة (للثقة المعرفية) بقيمة بلغت: (0.700) وضعيفة جدا بالنسبة (للثقة العاطفية) بقيمة بلغت: (0.060)، ومن هنا "**نثبت صحة الفرضية الرئيسية الثانية**".
- **الفرضة الرئيسية الثالثة:** أكدت عن وجود تأثير إيجابي بين جل أبعاد الأمن السيبراني في الخدمات الإلكترونية المصرفية، حيث تمتع بعد (التكنولوجيا المستخدمة) بأعلى مستوى من التأثير في العلاقة بقيمة بلغت: (0.790)، ما عدا بعد (احترام الخصوصية) كان تأثيره سلبي بقيمة بلغت: (1.045-)، ومن هنا **نثبت "صحة الفرضية الرئيسية الثالثة"**.
- **الفرضية الرئيسية الرابعة:** تبين لنا وجود تأثير غير مباشر لأبعاد الأمن السيبراني في الخدمات الإلكترونية المصرفية من خلال بعد الثقة المعرفية للعملاء كمتغير وسيط، تمتع فيها كل الأبعاد بأعلى مستوى من التأثير ما عدا بعد (احترام الخصوصية) كانت تأثيره سلبي بقيمة بلغت: (0.214-)، وكذا وجود تأثير غير مباشر لأبعاد الأمن السيبراني في الخدمات الإلكترونية المصرفية من خلال بعد الثقة العاطفية للعملاء كمتغير وسيط، تمتع فيها كل الأبعاد بأعلى مستوى من التأثير ما عدا بعد (التوافر والديمومة) كان تأثيره سلبي بقيمة بلغت: (1.211-)، وبعد (تتبع الأثر) بقيمة بلغت: (1.098-)، عليه يمكننا القول "**بصحة الفرضة الرئيسية الرابعة**".

✓ بعد رفض بعض العلاقات لضعف مستواهما، خلصت الدراسة إلى اقتراح نموذج معدل لمساهمة أبعاد الأمن السيبراني في الخدمات الإلكترونية المصرفية في ظل وجود ثقة العملاء كمتغير وسيط.

✓ **عليه ومن خلال ما سبق ذكره، يمكن إضافة بعض الاستنتاجات التي تخص موضوع الدراسة الميدانية:**

- البنك محل الدراسة يعمل وفق تدابير وإجراءات أمنية سليمة، تدخل ضمن اعتماد إستراتيجية شاملة فيما يتعلق بحماية مختلف معلومات وبيانات العملاء، من خلال تطويره التدريجي للبنى التحتية الرقمية، التوفر على شبكات اتصال، برامج وخوادم حديثة، مع استخدام تقنيات النسخ الافتراضي لجميع المعاملات الرقمية.
- بنك التنمية المحلية من بين أحدث البنوك في الجزائر بمواكبته لتكنولوجيا الإعلام والاتصال.
- يحظى بنك التنمية المحلية بصورة حسنة وسمعة طيبة لدى عملائه.
- هناك تصاعد تدريجي فيما يخص نسبة استعمال العملاء للبطاقات المصرفية الإلكترونية الخاصة ببنك التنمية المحلية مقارنة بما سجل في السنوات الماضية، لكنها تبقى ضعيفة مقارنة بالدول الأخرى المتقدمة، حيث ترجع إلى أسباب عديدة من بينها حداثة البنوك الجزائرية في تقديم الخدمات الإلكترونية، عدم مخاطرة الزبون الجزائري في الجانب المالي، ضعف الثقافة السيبرانية في المجتمع الجزائري، عدم كمال النصوص القانونية في الجزائر التي تقوم بردع الجرائم السيبرانية، ضعف الثقة في التعاملات الإلكترونية بصفة عامة وببطاقات الدفع الإلكترونية بصفة خاصة، عدم اتباع سياسة تسويقية فعالة من قبل إدارة البنوك فيما يخص الخدمات الإلكترونية المصرفية.
- الأمن السيبراني لبنك التنمية المحلية قوي بقوة شركة SATIM (Société Algérienne de Monétique D'automatisation des Transaction Interbancaires et) المسؤولة في الجزائر عن النقد الآلي والعلاقات التلقائية بين البنوك، هذه الأخيرة تعمل وفق اتفاقيات شراكة مع الشركات الأجنبية الكبرى المنتجة للبرمجيات والشبكات والنظم والأجهزة المتطورة ووسائل الحماية التقنية الجد متقدمة، وما يعكس حقيقة هاته القوة، قلة المشاكل التي تتعلق بالتعدي على البيانات كالاختراقات، التجسسات، حجب تقديم الخدمات الإلكترونية وغيرها من المشاكل التي تتعلق بعمليات السحب والدفع والتحويل ببطاقات الدفع الإلكترونية.
- ما دام أن الأمن السيبراني لبنك التنمية المحلية من مسؤولية شركة SATIM الأجنبية المستوردة للبرامج والشبكات والنظم من الدول الأجنبية المتقدمة، فالبنك في تبعية تكنولوجية، إذ يعتبرها العاقلون خطرا على سرية وخصوصية بيانات العملاء، إن لم نقل مجازفة لأمن وسلامة المؤسسة المصرفية.

مقترحات الدراسة:

- تسعى هذه الدراسة إلى طرح خبرات الباحثين السابقين من خلال متغيرات الدراسة (الأمن السيبراني، ثقة العملاء، الخدمات الإلكترونية المصرفية)، وذلك بهدف تقديم إطار مفاهيمي متكامل يمكن الاستفادة منه في تحسين أداء بنك التنمية المحلية غرداية في تقديم الخدمات الإلكترونية المختلفة عبر وسائل الدفع الإلكتروني.

- نوصي بنك التنمية المحلية باتخاذ تدابير وإجراءات تعتمد على عناصر الأمن السيبراني بصفة متكاملة كضرورة حتمية في العملية الإنتاجية للخدمات المصرفية الإلكترونية.

- ننصح بنك التنمية المحلية بالحرص أكثر على بناء المزيد من ثقة العملاء ببعديها (المعرفي والعاطفي) في الخدمات الإلكترونية المصرفية، مع العمل المستمر على التحسين من مستواها.

- الدراسة والتشخيص الجيد لتحديد ما من شأنه أن يسبب ضعف ثقة العملاء، ومعرفة عوامل تدني مستواها.

- انشاء آلية لتقييم الخدمات الإلكترونية المصرفية بعد استخدامها.

- الاعتماد على تكنولوجيا الذكاء الاصطناعي لزيادة فعالية الخدمات الإلكترونية المصرفية.

- نفضل اختيار أفضل النظم المعلوماتية وشبكات الاتصال ذات المواصفات القياسية وتطبيق معايير الجودة الدولية ISO لضمان سلامة أمن المعلومات والبيانات وحمايتها وأمن الشبكات من الاختراقات المحتملة، فضلا عن أهمية استخدام أنظمة التشغيل ذات المصدر المفتوح (open source software) مثل نظامي Linux وUnix التي تتميز بالاستقرار والأمنية المحكمة.

- نوجه البنك باتخاذ إجراءات احترازية للحماية والتحصين من أي تخريب أو سطو سيبراني أو أي خطر، بالمقابل العمل على التحديث المستمر للتقنيات والبرامج المضادة للاعتداءات والفيروسات، مع اعتماد الوسائل التقنية الحديثة للحماية فيما يخص (التشفير، التصديق الرقمي، البصمة الرقمية، جدار النار، تقنيات أخرى حديثة...الخ).

- اعتماد تقنيات النسخ الاحتياطي لمختلف العمليات الإلكترونية.

- نقترح للبنك تخصيص قسم خاص لأمن وحماية المعلومات والبيانات مهمته متابعة وتحديث برامج الحماية واكتشاف التهديدات والثغرات الأمنية قصد العمل على سدها وتقويمها.

- نلح على الاستثمار بكثافة في القوى البشرية من خلال تأهيل وتكوين وتدريب كوادر بشرية متخصصة في تقنيات الأمن السيبراني الأمن السيبراني ومجال الإلكترونيات من أجل أن تقف كحجر عثرة أمام أي محاولة لتهديد أمن البنك عامة وأمن تقديم الخدمات الإلكترونية المصرفية خاصة.

- نوصي البنك بالاعتماد على الكفاءات البشرية المحلية في مجال الأمن السيبراني من خلال صنع البرمجيات، النظم والشبكات ومختلف الوسائل التقنية بغية الخروج من التبعية التكنولوجية لشركة SATIM الأجنبية.

- العمل على توعية العملاء ومختلف شرائح المجتمع والمؤسسات بحجم المخاطر الناجمة عن الجرائم السيبرانية من خلال البرامج المسموعة والمرئية والندوات التثقيفية للرفع من مستوى ثقافتهم في مجال الأمن السيبراني في القطاع المالي والمصرفي.

- وضع إطار تعاون يضمن تبادل المعلومات والاستفادة من الخبرات والتجارب السابقة والاستشارات التي توفرها نظيراتها من المؤسسات والمكاتب المتخصصة في مجال الأمن السيبراني سواء المحلية أو الأجنبية.
- نوصي بالتكامل والتعاون بين البنوك الجزائرية في تنفيذ المبادرات التي تهدف إلى تعزيز الأمن السيبراني.
- نلح بانشاء إطار قانوني شامل يتماشى مع كل مستجدات الإجرام السيبراني لحماية حقوق العميل ضد العديد من المخاطر والتهديدات وحماية استخدام الخدمات الإلكترونية المصرفية.
- نقترح بتحميل المجرمين السيبرانيين عقوبات مشددة بغية ردعهم وحماية الفضاء السيبراني منهم.

آفاق الدراسة:

لقد أتاحت هذه الدراسة الولوج إلى مواضيع أخرى شيقة يمكن أن تكون محاور بحث مستقبلية تربط متغيرات الدراسة بجوانب عديدة في مجال التسويق مثل:

- دراسة هذا الموضوع من خلال توسيع قاعدة الاستبيان من خلال اعتماد عينات للعديد من البنوك العمومية منها والخاصة لندرس أوجه التشابه والاختلاف في مجال أمنها السيبراني.
- تأثير الذكاء الاصطناعي على فاعلية الأمن السيبراني للبيانات التسويقية للمؤسسات.
- دور الأمن السيبراني في الحد من مخاطر نظام المعلومات التسويقية، دراسة مقارنة بين مؤسسة خدمية وصناعية.
- مدى مساهمة الأمن السيبراني في بناء ثقة التسويق الدولي عبر قنوات التوزيع المباشرة وغير المباشرة.
- أثر الأمن السيبراني في جودة الخدمات الإلكترونية المصرفية.
- العوامل المؤثرة على الأمن السيبراني في الخدمات الالكترونية المصرفية عبر الهاتف النقال.
- اكتشاف العلاقة بين تدابير الأمن السيبراني ورضا الزبائن في الخدمات الإلكترونية المصرفية.
- أهمية الأمن السيبراني في تحقيق الميزة التنافسية من خلال التسويق الشبكي.
- مدى توافر الوعي بالأمن السيبراني لدى عملاء البنوك العمومية الجزائرية.
- متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات المصرفية وانعكاساتها على مردودية البنوك.
- تأثير تصور العملاء لبعدي الأمن السيبراني واحترام الخصوصية على قبول الخدمات الإلكترونية المصرفية.
- شهادة التصديق الإلكتروني كآلية لتعزيز الثقة الرقمية في الخدمات الإلكترونية المصرفية.
- مساهمة بعدي سرية البيانات واحترام الخصوصية كمؤشر لجودة الخدمات الالكترونية المصرفية على ولاء العملاء.
- أثر أبعاد الأمن السيبراني على سهولة استخدام الخدمات الإلكترونية المصرفية من وجهة نظر موظفي البنوك الخاصة.

- تأثير المخاطر والتهديدات السيبرانية على تبني المستهلك الإلكتروني الخدمات الإلكترونية.
- استكشاف أهم العوامل المؤثرة في العلاقة بين الثقة واستخدام الخدمات البريدية الإلكترونية.

هذه الآفاق البحثية هي مجرد نماذج يمكن توسيعها بحسب اهتمامات الباحث أو المؤسسة، بحيث يمكن أن تقدم هذه الدراسات تحسينات أو حلول من المفترض اللجوء إليها بغية تطوير وتحسين الأداء وتحقيق الأهداف المرجوة.

قائمة المراجع

أولا: المصادر والمراجع باللغة العربية

- **I. الكتب:**

1. القرآن الكريم.

2. أحمد بوراس، سعيد بريكة، **أعمال الصيرفة الإلكترونية الأدوات والمخاطر**، دار الكتاب الحديث، القاهرة، مصر، الطبعة الأولى، 2014.

3. أحمد سفر، **العمل المصرفي الإلكتروني في البلدان العربية**، المؤسسة الحديثة للكتاب، طرابلس، لبنان، دون طبعة، 2006.

4. أسامة حسام الدين، **مقدمة في الأمن السيبراني 0.2**، كلية علوم وهندسة الحاسبات، أكاديمية سيسكو، 2017.

5. أسامة عبد الله قايد، **الحماية الجنائية للحياة الخاصة وبنوك المعلومات دراسة مقارنة في القانون الفرنسي والأمريكي والمصري وفقا لآخر التعديلات التشريعية**، دار النهضة العربية، القاهرة، بدون رقم طبعة، 2015.

6. بسام شيخ العشرة، حنان مليكة، **التجارة الإلكترونية**، نشر الجامعة الافتراضية السورية، 2018.

7. خديجة عتيق، **واقع التسويق المصرفي في البنوك وأثرها على رضا العملاء**، دار خالد اللحياني للنشر والتوزيع، مكة، السعودية، 2016.

8. بيتر بيسيل، **الكون الرقمي الثورة العالمية في الاتصالات**، مؤسسة هنداوي للنشر، المملكة المتحدة، 2017.

9. خليفة إيهاب، **القوة الإلكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الإنترنت**، دار العربي للنشر، 2017.

10. ذيب بن عايض القحطاني، **أمن المعلومات**، دار النشر لمدينة الملك بن عبد العزيز للعلوم والتقنية KACST، الرياض، السعودية، 2015.

11. رستم هاشم محمد، **جرائم الحاسب المستحدثة**، دار الكتب القانونية، مصر، الطبعة الأولى، 2015.

12. سعد غالب ياسين، **نظم إدارة قواعد البيانات**، دار اليازوري العلمية للنشر والتوزيع، عمان، الأردن، 2010.

13. سمير توفيق صبرة، **التسويق الإلكتروني**، دار الاعصار العلمي للنشر والتوزيع، عمان، الأردن، الطبعة الأولى، 2010.

14. سوسن زهير المهتدي، **تكنولوجيا الحكومة الإلكترونية**، دار أسامة للنشر والتوزيع، عمان، الأردن، الطبعة الأولى، 2011.

15. سيناس كوستيجان، **الأمن السيبراني منهج مرجعي عام**، أكاديمية الدفاع الكندية، كندا، 2016.

16. صلاح الدين حسن السيسي، **التجارة الدولية والصيرفة الإلكترونية، النظريات والسياسات**، دار الكتاب الحديث، القاهر، مصر، 2014.

17. صلاح الدين محمد علي، **كيفية توفير عنصر الأمن والسرية للمعاملات المصرفية عبر شبكة الإنترنت في المصارف السودانية**، دار المنظومة، العدد 73، 2016،

18. طارق إبراهيم الدسوقي عطية، **الأمن المعلوماتي**، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، 2015.

19. عامر إبراهيم قنديلجي، **التجارة الإلكترونية وتطبيقاتها**، دار الميسرة للنشر والتوزيع والطباعة، عمان، الأردن، الطبعة الرابعة، 2015.

20. عبد الصمد حوالف، **النظام القانوني لوسائل الدفع في الجزائر، دراسة مقارنة**، دار الجامعة الجديدة، الإسكندرية، مصر، 2016.

21. عزة علي آل كباس، **التخزين السحابي**، 2017.

22. علي الرمحي مرعى، **الحرب السيبرانية ومتطلبات الأمن القومي الجديدة**، المركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية، برلين، ألمانيا، الطبعة الأولى، 2022.

23. علي بن عيدروس بن علي البار، **الأمن السيبراني رؤية 2030**، نشر كلية ينبع الجامعية، العزيزية، السعودية، 2022.

24. علي عبد المحسن الجبوري، **الوسائل الحديثة للدفع في إطار التجارة الإلكترونية**، دار النهضة العربية، القاهرة، مصر، الطبعة الأولى، 2019.

25. غانم حجاج، **التحليل العاملي في العلوم الإنسانية والتربوية نظريا وعمليا**، عالم الكتب للنشر، القاهرة، مصر، 2013.

26. غسان سابا، **أمن الشبكات والبنية التحتية المعلوماتية**، نشر وتوزيع الجامعة الافتراضية السورية، سوريا، 2018.

27. فؤاد أمين السيد محمد، **جرائم مراقبة المراسلات الإلكترونية، دراسة مقارنة**، دار النهضة العربية، القاهرة، مصر، الطبعة الأولى، 2016.

28. محمد أحمد سليمان، **التسويق وتكنولوجيا الاتصالات**، دار زمزم للنشر والتوزيع، الأردن، الطبعة الأولى، 2013.

29. محمد بن احمد السديري، **التجارة الإلكترونية تقنيات واستراتيجيات التطبيق**، 2023.

30. محمد عبد حسين الطائي، "**التجارة الإلكترونية، المستقبل الواعد للأجيال القادمة** "، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2010.

31. محمد محمود العمري، **مدخل إلى الأمن السيبراني**، دار زهران للنشر والتوزيع، عمان، الأردن، 2020.

32. مرتضى محمد عبد اللطيف، **دور قطاع تكنولوجيا المعلومات والاتصال في التنمية الاقتصادية**، المكتب العربي للمعارف، القاهرة، مصر، الطبعة الأولى، 2014.

33. مركز هردو، **الجريمة الإلكترونية وحجية الدليل الرقمي في الإثبات الجنائي**، الناشر مركز هردو، القاهرة، مصر، 2014.

34. مصطفى كافي، **النقود والبنوك الإلكترونية**، دار رسلان، دمشق، سوريا، 2012.

35. منى الأشقر جبور، **السيبرانية هاجس العصر**، نشر المركز العربي للبحوث القانونية والقضائية، بيروت، لبنان، 2017.

36. منى الأشقر جبور، محمود جبور، **البيانات الشخصية والقوانين العربية**، دراسات وأبحاث المركز العربي للبحوث القانونية والقضائية (الأمن المعلوماتي والأمن القانوني)، بيروت، لبنان، 2019.

37. منير نوري، **سلوك المستهلك المعاصر**، ديوان المطبوعات الجامعية للنشر والتوزيع، الجزائر، 2013.

38. ناجي ذيب معلا، **الأصول العلمية للتسويق المصرفي**، دار المسيرة للنشر والتوزيع والطباعة، عمان، الأردن، الطبعة الأولى، 2015.

39. نادية شبانة، السعيد بريكة، **البنوك الإلكترونية الواقع والأفق**، دار الكتاب الحديث، القاهرة، مصر، الطبعة الأولى، 2016.

40. نواف المنج، **أمن المعلومات والشبكات**، قسم الشبكات الكهربائية، مكتبة نور الرقمية، 2020.

41. نوري منير، **نظام المعلومات المطبق في التسيير**، ديوان المطبوعات الجامعية، طبقة الأولى، الجزائر، 2015.

42. هلال عبد الله أحمد، **اتفاقية بودابست لمكافحة الجرائم المعلوماتية (معلقا عليها)**، دار النهضة العربية، دار الكتب القانونية للنشر، القاهرة، مصر، الطبعة الأولى، 2008.

43. هيثم السيد أحمد عيسى، **نشأة العقود الذكية في عصر البلوكشن**، دار النهضة العربية للنشر والتوزيع، القاهرة، الطبعة الأولى، 2021.

44. وزارة التعليم للملكة العربية السعودية، **علم البيانات**، مسار الثانية ثانوي، الناشر شركة تطوير للخدمات التعليمية، 2022.

45. يوسف أنور، **صفوة لينكس لباحثي الأمن السيبراني**، مكتبة نور كتب، جامعة الأزهر، مصر، 2019.

46. يوسف أنور، **معجم قدس للأمن السيبراني**، مكتبة نور كتب، جامعة الأزهر، مصر، 2018.

47. يوسف حسن يوسف، **البنوك الإلكترونية**، المركز القومي للإصدارات القانونية، القاهرة، مصر، الطبعة الأولى، 2012.

- **II. البحوث الجامعية:**

أ) أطروحات دكتوراه:

1. آسية بن أحمد، **أثر المرونة الإستراتيجية على جودة فاعلية الأداء وتنافسية المؤسسة، دراسة تطبيقية على شركة الاتصالات موبيليس**، أطروحة دكتوراه علوم تجارية، جامعة الجيلالي اليابس سيدي بلعباس، كلية العلوم الاقتصادية التجارية وعلوم التسيير، 2017.
2. خالد سحنون، **تأثير تكنولوجيا المعلومات على مردودية البنوك**، أطروحة مقدمة لنيل شهادة الدكتوراه، تخصص علوم اقتصادية، جامعة أبو بكر بلقايد، تلمسان، الجزائر، 2016.
3. صالح أحمد عبود العدوان، **أثر جودة الخدمات المصرفية الإلكترونية في تعزيز الأداء** – دراسة على المصارف التجارية الأردنية، أطروحة دكتوراه، جامعة العلوم الإسلامية العالمية، عمان، الأردن، 2015.
4. صليح بونفلة، **النظام القانوني للعمليات المصرفية الإلكترونية**، أطروحة مقدمة لنيل شهادة الدكتوراه تخصص قانون الأعمال، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة 8 ماي 1945 قالمة، الجزائر، 2021.
5. عبد اللطيف حمام، عبد الشافي حنفي معوض، **الحماية الجنائية للبرامج والبيانات المعالجة إلكترونيا، دراسة مقارنة**، رسالة قدمت لنيل درجة الدكتوراه حقوق، جامعة القاهرة، مصر، 2017.
6. ماجدة بن صالح، **"العوامل المؤثرة على ثقة العملاء في الخدمات المصرفية الالكترونية – دراسة حالة البنوك الجزائرية"**، أطروحة دكتوراه، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، قسم علوم التسيير، شعبة علوم التسيير، جامعة 8 ماي 1945 ولاية قالمة، الجزائر، 2021.
7. مراد ماشوش، **الجرائم الاقتصادية وسبيل مكافحتها -الجهود الدولية لمكافحة الإجرام السيبراني**، دكتوراه في القانون العام الاقتصادي، كلية الحقوق والعلوم السياسية جامعة غرداية، الجزائر، سنة 2017/2016.
8. وفاء حلوز، **تدعيم جودة الخدمة البنكية وتقييمها من خلال رضا العميل**، أطروحة دكتوراه في البنوك، كلية العلوم الاقتصادية والتجارية والتسيير، جامعة أبو بكر بلقايد-تلمسان، الجزائر، 2014.
9. يوسف بوغرارة، **الأمن السيبراني الإستراتيجة الجزائرية للأمن والدفاع في الفضاء السايبيري**، دكتوراه في القانون العام، كلية الحقوق والعلوم السياسية مستغانم، الجزائر 2017.

ب) رسائل ماجستير:

1. ابراهيم موصلي، **العوامل المؤثرة في سلوك العملاء تجاه الخدمات الإلكترونية للمصارف، دراسة ميدانية**، رسالة أعدت لنيل درجة ماجستير في إدارة الأعمال، جامعة حلب، كلية الاقتصاد، قسم إدارة الأعمال، 2011.

2. أحمد زياد أدلي، **العوامل المؤثرة في نية واستخدام التعلم الإلكتروني–دراسة ميدانية في شركات القطاع الصناعي في سوريا**، رسالة أعدت لنيل درجة ماجستير في علوم الإدارة تخصص الموارد البشرية، قسم الموارد البشرية، المعهد العالي لإدارة الأعمال، دمشق، سوريا، 2019.

3. بلال راحو، **الخدمات المصرفية الإلكترونية وأثرها في تحسين جودة الخدمات المصرفية الإلكترونية، دراسة تطبيقية لأراء عينة من الزبائن والإداريين العاملين بالمصارف التجارية العاملة في مدينة البليدة**، رسالة ماجستير في العلوم الاقتصادية، تخصص مالي ونقود، جامعة الدكتور يحي فارس المدية، الجزائر، 2015.

4. حاج محمد مخرمش، **دور الصيرفة الإلكترونية في تحقيق الميزة التنافسية للبنوك التجارية**، رسالة ماجستير تخصص مالية وبنوك، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة ورقلة، الجزائر، 2018.

5. حنين جميل أبو الحسن، **الإطار القانوني لخدمات الأمن السيبراني، دراسة مقارنة**، رسالة ماجستير في القانون الخاص، كلية الحقوق، جامعة الشرق الأوسط، عمان الأردن، 2021.

6. زهرة خلوط، **التسويق الابتكاري وأثره على بناء ولاء الزبائن**، رسالة ماجستير، تخصص تسويق، الجزائر، 2014.

7. سعد محمد أبو كميل، **تطوير أدوات الرقابة الداخلية لهدف حماية البيانات المعدة إلكترونيا، دراسة تطبيقية**، رسالة ماجستير، غزة، فلسطين، 2011.

8. سيد ماهر بدوي عبد الله، **أثر ثقة العميل في المؤسسة المصرفية على قبول التعامل المصرفي عبر الإنترنت**، رسالة ماجستير، كلية التجارة، قسم إدارة الأعمال، جامعة القاهرة مصر، 2013.

9. عبد الرحمن العتيبي بن بجاد شارع، "**دور الأمن السيبراني في تعزيز الأمن الانساني**"–دراسة ميدانية لمجموعة من المحطات التابعة لشركة أرامكو لتكرير النفط، السعودية، رسالة ماجستير، قسم الأمن الإنساني، كلية العلوم الاستراتيجية، جامعة نايف للعلوم الأمنية، السعودية، 2017.

10. عراجي أنديرا، **القوة في الفضاء السيبراني فصل عصري من التحدي والاستجابة**، رسالة ماجستير، كلية الحقوق والعلوم السياسية والإدارية، لبنان، 2016/2015.

11. كريمة صراع، **واقع وآفاق التجارة الإلكترونية في الجزائر**، رسالة ماجستير، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، المدرسة الدكتورالية للاقتصاد وإدارة الأعمال، وهران، الجزائر، 2014.

- **III. محاضرات:**

1. ابراهيم بختي، **محاضرات في مقياس الصيرفة الإلكترونية**، اختصاص مالية وبنوك، قسم العلوم الاقتصادية، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة قاصدي مرباح ورقلة، الجزائر، 2018.

- **IV. المقالات العلمية:**

1. أبو القاسم الأخضر حمدي، **دور التعلم غير الرسمي في تنمية كفاءات الموارد البشرية**، مجلة دراسات، جامعة الأغواط، العدد 43، جوان 2016.
2. أمحمد بوزيان تيغزة، **توجهات حديثة في تقدير صدق وثبات درجات أدوات القياس**، مجلة العلوم النفسية والتربوية، جامعة الشهيد حمة لخضر، الوادي الجزائر، المجلد 04 العدد 01، مارس 2017، ص 10.
3. أحمد نور الدين عمرو، **"أثر المخاطر المدركة على استخدام الخدمات المصرفية الالكترونية في مصر: الدور الوسيط لتوقعات الثقة –دراسة ميدانية"**، مجلة جامعة الإسكندرية للعلوم الإدارية، كلية التجارة، جامعة الإسكندرية مصر، المجلد 59، العدد 3، 2022.
4. اسكندر سرجيوس، أنطوان، **تأثير جودة الموقع الإلكتروني على النية نحو الشراء: في ظل الدور الوسيط للثقة في الموقع والاتجاه نحوه**، مجلة جامعة الإسكندرية للعلوم الإدارية، العدد 68، رقم 6، 2021.
5. الزهرة برة وجميلة حميدة، **"شهادة التصديق الإلكتروني كآلية لتعزيز الثقة في المعاملات الالكترونية"**، مجلة العلوم القانونية والسياسية، جامعة لونيسي علي العفرون، البليدة 2، الجزائر، المجلد 10، العدد 01، 2019.
6. الشيخ ساوس ومحمد فودو، **نمذجة المعادلات الهيكلية باستخدام المربعات الصغرى الجزئية مثال تطبيقي باستخدام R في بحوث المحاسبة والتدقيق**، مجلة معهد العلوم الاقتصادية، المجلد 22، عدد 01، 2019، ص ص 179-196.
7. أنس محمد عبد الغفار سلامة، **إثبات التعاقد عبر تقنية البلوك تشين**، مجلة العلوم القانونية والاجتماعية، المجلد 05، العدد 02، جوان 2020.
8. بسمة كحول، سعيدة طيب، **أهمية استخدام المواصفة القياسية الدولية الـ ISO 27001 لإدارة أنظمة أمن المعلومات**، مجلة المستقبل للدراسات الاقتصادية المعمقة، المجلد رقم 01، العدد 01، ديسمبر 2018.
9. جمال بوزادية، **الإستراتيجية الجزائرية في مواجهة الجرائم السيبرانية الآفاق والتحديات**، مجلة العلوم القانونية والسياسية الجزائر، المجلد 10، العدد 01، أفريل 2019.
10. جهاد أحمد السيد محمد، **أهمية الشبكات في مؤسسات الدفع الإلكتروني**، إصدارات المركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية، الجزء الأول، برلين، ألمانيا، 2022.
11. حسين القاضي، مادلين عبود، سمى سنكري، **واقع تقنيات الدفع الإلكتروني في المصارف السورية**، مجلة جامعة ترشين للبحوث والدراسات العلمية، سوريا، العدد 5، 2012.

12. حسن نجيب الرواش، رعد مشعل محمد التل، صالح إبراهيم العمر، **"محددات استخدام الخدمات المصرفية الإلكترونية في الأردن من وجهة نظر العملاء"**، المجلة العالمية للاقتصاد والأعمال الأردن، المجلد 08، العدد 03، 2020.

13. حمزة جيلاني تومي، موراد تهتان، **أثر كل من حجم البنك، الربحية والسيولة عل هيكل رأس المال في البنوك الجزائرية**، المجلة الجزائرية للاقتصاد والمالية، العدد 9، أفريل 2018.

14. خالد ظاهر عبد الله جابر السهيل المطيري، **دور التشريعات الجزائية في حماية الأمن السيبراني بدول مجلس التعاون الخليجي**، مجلة البحوث الفقهية والقانونية، العدد 28، يوليو 2022.

15. ربيعة يبدري، **دور الأمن السيبراني في حماية المعاملات المالية المصرفية المبرمة في الشكل الإلكتروني**، إصدارات المركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية، الجزء الأول، برلين، ألمانيا، 2022.

16. سعدية مزيان، **أثر ثقة الزبائن على ولائهم للمؤسسات الصحية الخاصة، دراسة حالة عينة عيادة نوميديا أم البواقي**، مجلة جديد الاقتصاد، المجلد 17، العدد 01، 2022.

17. سعيد زيوش، **التجارة الإلكترونية وآليات حماية خصوصية المستهلك الجزائري**، مجلة هيرودوت للعلوم الإنسانية والاجتماعية، بريكة، باتنة، الجزائر، المجلد 7، العدد 25، 2023.

18. سلمى بلمهدي، سمرة دومي، **دراسة مستوى ثقة الزبائن في البنوك التجارية–دراسة مقارنة بين البنوك العمومية والخاصة**، مجلة اقتصاديات الأعمال والتجارة، المجلد 6، العدد 2، 2021.

19. صندوق النقد العربي، **سلامة وأمن المعلومات المصرفية الإلكترونية، اللجنة العربية للرقابة المصرفية**، أمانة مجلس محافظي المصارف المركزية ومؤسسات النقد العربية، العدد 76، أبو ظبي، الإمارات العربية المتحدة، 2017.

20. عبد اللطيف عامر، مصطفى صلاح عمر، أكرم نعيم قاسم، **تأثير التسويق الفيروسي في ثقة الزبون: دراسة تحليلية في شركة آسيا سيل**، مجلة التقنيات، المجلد 05، رقم 01، 2023.

21. عمار بوحوش، محمد الذنيبات، **مناهج البحث العلمي وطرق إعداد البحوث**، الطبعة السادسة ديوان المطبوعات الجامعية بن عكنون، الجزائر، 2018.

22. عمر توفيق عبد الرحيم، ثابت حسان ثابت، عمر سالم عز، **تحليل العوامل المؤثرة على تعزيز ثقة الزبون في استخدام الخدمات المصرفية الذكية: تطبيقات الهواتف الذكية انموذجا**، مجلة العلوم المالية والمحاسبة، 2022.

23. عياش زبير، **تطوير وعصرنة الخدمات البنكية في ظل التوجه نحو اقتصاد المعرفة حالة الجزائر**، مجلة ميلاف للبحوث والدراسات، العدد الخامس، جامعة العربي بن مهيدي أم البواقي، 2017/06/25.

24. فاطمة مصفح، زينة آيت علي، **مفهوم الدفع الإلكتروني وتمييزه عن الدفع التقليدي**، مجلة البحوث والدراسات القانونية والسياسية، المجلد 11، العدد 02، 2022.

25. فريدة حمودي، **الأمن المعلوماتي في الجزائر بين التطورات التكنولوجية وضعف البيئة الرقمية، المجال المصرفي نموذجا**، مجلة جيل الأبحاث القانونية المعمقة، لبنان، العدد 41، 2020.

26. لطفي أمين بلفرد، **الفضاء السيبراني: هندسة وفواعل**، المجلة الجزائرية للدراسات السياسية، العدد الخامس، 2016.

27. لمين علوطي، **تحديات الأمن الإلكترونية في المؤسسة، مجلة أبحاث اقتصادية وإدارية**، العدد 06، 2009.

28. محمد اسماعيل، "**الأمن السيبراني في القطاع المصرفي**، موجز سياسات، صندوق النقد العربي، العدد 04، جويلية 2019.

29. محمد الشرفي، رزيني عبد الله، فادي حرز الله، عماد أبو شنب، "**تأثير ثقة العملاء وتصورهم للأمن والخصوصية عند قبول الخدمات المصرفية عبر الانترنت**"، مجلة الإدارة الصناعية، جامعة ماليزيا، المجلد 04 جوان 2018.

30. محمد المهدي الأمير، عبد الرحمان يوسف الخليفة، صلاح علي أحمد محمد، **أثر التحول لنظام المحاسبة الرقمية على خاصية التمثيل الصادق للمعلومات المحاسبية في ظل مبادئ ومعايير موثوقية الموقع الإلكتروني**، مجلة أرصاد الراسات الاقتصادية والإدارية، السودان، المجلد 04، العدد 02، ديسمبر 2021.

31. محمد بن أشنهو، قريش بن علال، **العوامل المؤثرة على ثقة الزبون، دراسة إمبريقية باستعمال طريقة المعادلات البنائية**، مجلة المالية والأسواق، المجلد 02، العدد 02، 2015.

32. محمد بوزيان تيغزة، **التحليل العاملي الاستكشافي والتوكيدي**، دار المسيرة للنشر والتوزيع والطباعة، عمان–الأردن، الطبعة الأولى، 2012.

33. محمد بوكبشة، **إستراتيجية الجزائرية للأمن والدفاع في الفضاء السايبيري**، مجلة الدراسات الإفريقية وحوض النيل، العدد 3، المجلد الأول، المركز الديمقراطي العربي، برلين، ألمانيا، سبتمر 2018.

34. محمد بوكبشة، **مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة**، مجلة الجيش، العدد 651، 2017.

35. محمد عصمان، شريف مهدي، "**الثقة والأمان في الخدمات المصرفية الالكترونية في البنوك التجارية السعودية: آراء السعوديين مقابل غير السعوديين**"، مجلة إدارة الأعمال، المجلد 5، العدد 14، 2011.

36. محمد علي خليل السميرات، **العوامل المؤثرة في استخدام الخدمات البنكية الإلكترونية عبر الهاتف المحمول من وجهة نظر العملاء: دراسة ميدان إقليم الجنوب–الأردن**، مجلة جامعة الشارقة للعلوم الإنسانية والاجتماعية، المجلد 14، العدد 1، 2017.

37. مروة فتحي السيد البغدادي، **"اقتصاديات الأمن السيبراني في القطاع المصرفي"**، مجلة البحوث القانونية والاقتصادية، مدرسة الاقتصاد والمالية العامة بالمعهد المصري، أكاديمية الإسكندرية للإدارة والمحاسبة، الجامعة المصرية، الإسكندرية، مصر، المجلد 11، العدد 2، الرقم المسلسل للعدد 76، 2021.

38. مليكة درياد، **المساس بأنظمة المعالجة الآلية للمعطيات**، مجلة حوليات، جامعة الجزائر 1، العدد 33، الجزء الأول، مارس 2019.

39. مني عبد الله السمحان، **متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود**، مجلة كلية التربية، جامعة المنصورة، العدد 11، جويلية 2020.

40. منير عبد الله مفلح البيشي، **"الأمن السيبراني في الجامعات السعودية وأثره في تعزيز الثقة الرقمية من وجهة نظر أعضاء هيئة التدريس: دراسة على جامعة بيشة"**، مجلة الجامعة الإسلامية للدراسات التربوية والنفسية، جامعة المملكة العربية السعودية، المجلد 29، العدد 6، 2021.

41. نبيل خادم، **دور بناء الثقة في تطوير المعاملات الرقمية**، فرنسا انموذجا، مجلة الفكر القانوني والسياسي، المجلد 05، العدد 01، 2021.

42. نور الدين بربار، محمد هشام قلمين، **دور الأمن المعلوماتي في تفعيل نشاط الصيرفة الإلكترونية**، مجلة الاقتصاد والتنمية، مخبر التنمية المحلية المستدامة، المدية، العدد 02، 2014.

43. نور الهدى قادري، بوزيان مكلكل، **التشفير بتقنية البلوك تشين ودوره في حماية المعاملات الإلكترونية**، مجلة القانون العام الجزائري والمقارن، المجلد 08، العدد 02، ديسمبر 2022.

44. هجيره ديدوش، حريزي عبد الغني، **واقع الخدمات المصرفية الإلكترونية بالبنوك الجزائرية، مجلة استراتيجيات التحقيقات الاقتصادية والمالية**، المجلد 04، العدد 01، 2022.

45. وليم سلامة شيري، أنسيمون كمال عزيز، أحمد مصطفى الشيخ، **الأمن السيبراني للخدمات المالية والمصرفية**، إصدارات المركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية، الجزء الأول، برلين، ألمانيا، 2022.

46. يوسف بوغرارة، **إستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبيري**، مجلة الدراسات الإفريقية وحوض النيل، العدد 3، المجلد الأول، المركز الديمقراطي العربي، برلين، ألمانيا، سبتمر 2018.

- **V. التظاهرات العلمية:**

أ) الملتقيات الوطنية:

1. محمد بن عزة، جليلة زويهري، **واقع المصارف الجزائرية في تطبيق نظام الدفع الإلكتروني**، دراسة حالة بنك الفلاحة والتنمية الريفية BADR، الملتقى العلمي الرابع حول: "عصرنة نظام الدفع في البنوك الجزائرية وإشكالية اعتماد التجارة الإلكتروني في الجزائر المركز الجامعي خميس مليانة، عين الدفلى، 2011.

2. ياسمينة ياسع، عبد الرحمان تومي، **دراسة تحليلية لتطور نشاط الصيرفة الإلكترونية في الجزائر من خلال أهم المؤشرات–تحليل مقارن**، "مداخلة مقدمة ضمن فعاليات الملتقى الوطني الثامن حول آليات تفعيل وسائل الدفع الحديثة في النظام المالي والمصرفي الجزائري"، تنظيم كلية العلوم الاقتصادية والتجارية وعلوم التسيير جامعة البويرة، الجزائر، يومي 14/13 مارس، 2017.

ب) الملتقيات الدولية:

1. سمير بارة، **الدفاع الوطني والسياسات الوطنية للأمن السيبراني في الجزائر: الدور والتحديات**، الملتقى الدولي حول سياسات الدفاع الوطني، جامعة قاصدي مرباح ورقلة، كلية الحقوق والعلوم السياسية، 2017/01/31.
2. مريزق عدمان، عماد بوقلاشي، **الأمن المعلوماتي في ظل التجارة الإلكترونية، إشارة إلى حالتي تونس والجزائر**، مداخلة ضمن فعاليات الملتقى العلمي الدولي الرابع حول عصرنة نظام الدفع في البنوك الجزائرية وإشكالية اعتماد التجارة الإلكترونية في الجزائر، عرض تجارب دولية، منشورة، المركز الجامعي خميس مليانة، يومي: 26-27 أفريل 2011.
3. نذير غانم، معمر جميلة، ريحان عبد الحميد، عنكوش نبيل، **الثقة الرقمية ضمن إستراتيجية الجزائر الإلكترونية 2013 واقعها ودورها في إرساء مجتمع المعرفة**، أعمال المؤتمر الثالث والعشرون: الحكومة والمجتمع والتكامل في بناء المجتمعات المعرفية العربية، ج 1، الدوحة، قطر، 2012.
4. هيثم المسيري، ندوة الخدمات البنكية الإلكترونية الشاملة (رؤية مستقبلية)، كتاب أعمال الملتقى العربي الأول حول: **المصارف الإسلامية، الواقع والتحديات**، المنعقد يومي: 25-29 نوفمبر 2007، الشارقة، الإمارات العربية المتحدة، نشر عن المنظمة العربية للتنمية الإدارية، القاهرة، مصر، 2011.
5. ربيعة يبدري، **"دور الأمن السيبراني في حماية المعاملات المالية المصرفية"**، مداخلة بالمؤتمر الدولي العلمي استخدام التكنولوجيا في المؤسسات المالية والمؤسسات الناشئة، إصدار المركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية، برلين، ألمانيا، يومي: 04 -05-جوان 2022.

ت) الندوات:

1. كليمان سارة غران، **التعلم الرقمي: التربية والمهارات في العصر الرقمي**، الندوة الاستشارية المعنية بالتعلم الرقمي التي عقدت كجزء من برنامج معهد كورشام للقيادة الفكرية: (Corsham Institute Thought Leadership Programme)، 2018.

2. هيثم المسيرى، **تقنيات البنوك الإلكترونية**، ندوة الخدمات الإلكترونية الشاملة (رؤية مستقبلية) القاهرة، جمهورية مصر العربية، يومي: 25-29 نوفمبر 2007.

- **VI. القوانين والمراسيم:**

1. الأمر رقم: 11-21، المتضمن **قانون الإجراءات الجزائية، استحداث القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الاعلام**، المؤرخ في: 25 أوت 2021.
2. القانون رقم: 03-16، المتضمن **البصمات الجنائية في الإجراءات الجزائية لتحديد هوية الأشخاص وتعزيز الجهات القضائية بأربعة محاكم خاصة**، الصادر بتاريخ: 2016/06/19.
3. القانون رقم: 04-09 المتضمن **القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها**، ج.ر.ج.ج، عدد 4، الصادر بتاريخ: 05-08-2009.
4. القانون رقم:04-09، المتضمن **القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها**، الفصل السابع مكرر المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات من قانون العقوبات الجزائري.
5. القانون رقم: 04-15 المتضمن **الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات**، المتمم للأمر رقم: 66-156 المتضمن لقانون العقوبات ج.ر.ج.ج، عدد 71، الصادر بتاريخ: 05-11-2004.
6. القانون رقم: 04-18، المؤرخ في: 10-05-2018 الذي **يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية**، ج.ر.ج.ج، عدد 27، صادر بتاريخ 27 شعبان عام 1439 ه الموافق ل 13 ماي 2018.
7. القانون: 05-18، المتضمن **قانون التجارة الإلكترونية**، المؤرخ في 24 شعبان عام 1439 الموافق 10 ماي سنة 2018.
8. قانون بنك الجزائر رقم: 07-05 المؤرخ في 28-12-2005، المتضمن **أمن أنظمة الدفع**، ج.ر.ج.ج، عدد 37، الصادر بتاريخ: 04-06-2006.
9. القانون رقم: 18-04، المتعلق **بالقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية**، المؤرخ في: 24 شعبان 1439 الموافقـ 10ماي 2018، المادة 10، ج.ر.ج.ج، الباب الأول، القسم الثاني، العدد 27، الصادر بتاريخ: 13 ماي 2018.

- **VII. التقارير:**

1. الاتحاد الدولي للاتصالات (ITU)، **تقرير صادر عن الأمم المتحدة**، 2011.

2. الاتحاد الدولي للاتصالات (ITU)، **دليل الأمن السيبراني للبلدان النامية**، طبع في جنيف سويسرا، 2006.

3. إياد عماد علي، **الحوسبة السحابية**، دائرة تقنية المعلومات والاتصالات، البنك المركزي العراقي، 2023.

- **VIII. الجرائد:**

1. فهد الحويماني، "**الاستثمار في شركات الأمن السيبراني**"، جريدة العرب الاقتصادية الدولية بالسعودية"، 21-09-2021.

2. طارق عباس، **يجب إدماج حماية البيانات في ثقافة الشركة**، جريدة البيان الإماراتية، العدد 13794، 25 مارس 2018.

ثانيا: المراجع باللغة الأجنبية:

- **I. Books:**

1. Ayten Okusz and all, **Trust in the Information Systems Discipline in Trust and Communication in a Digitized World: Models and Concepts of Trust Research**, Springer International Publishing Switzerland, 2016.
2. Chris Halliburton, **The Role of Trust in Consumer Relationships**, ESCP Europe Business School, 2010.
3. Christof Paar and Jan Pelzl, **Understanding Cryptography**, Springer Verlag Berlin Heidelberg, 2010.
4. Connolly Barry، **Digital Trust: Social Media Strategies to Increase Trust and Engage Customers**, Bloomsbury Publishing, 2020.
5. Daniel Ventre, **Cyberattaque et cyber défense,** La Voisier, Paris, 2011.
6. Devon Johnson, Kent Grayson, **Sources and Dimensions of Trust in Service Relationships, in T.A Lacobucc, Hanbook of Services Marketing and Management**, New yourk: SAGE Publication, Inc, 2000.
7. D'Silva Derryl, Filkova Zuzana, Packer Frank, Tiwari Siddharth**, The Design of digital Financial Infrastructure: Lessons from India,** BIS Paper, 2019.

8. Fernandez Toro, Sécurité Opérationnelle, **"conseil pratique pour sécuriser le système d'information"**, Eyrolles, 2016.
9. Filho Figueiredo, Silva Junior, Rocha Enivaldo, **What is R2 all about, Leviathan (Sao Paulo)**, N 3, 2011.
10. Hair joseph, **Partial Least Squares Structual Equation Modeling PLS-SEM Using R 1ed**, Switzerland: Springer Cham, 2021.
11. Hair Joseph, Hult Tomas, Marko Sarstedt, Hollingsworth**, A Primer on Partial Least Squares Structural Equation Modeling PLS-SEM**, 2ed, Sag, Thousand Oaks, CA 2017.
12. Héla Chérif Benmiled, **La confiance en Marketing**, Recherche et Application en Marketing, N 4, Université Paris, France, 2012.
13. Joanna Defranco, **What Every Should Know About Cyber Security and Digital Forensics**, Boka Ranton: CRC press, 2014.
14. Junger Moritz, Mietzner Mark, **Banking Goes Digital: The Adoption of FinTech Services by German Households**, Finance Research Letters, 2020.
15. Kaushik Kumar Panigrahi, **Information Security and Cyber Law**, Published by Tutorials Point, India, 2015.
16. Ken Wong Kay, **Partial Least Squares Srtuctural Equation Modeling (PLS-SEM) Technique Using Smart PLS**, Marketing Bulletin, Vol 24, N 1, 2013.
17. Koh Francis, Phoon Kok, Ha Cao, **Digital Financial Inclusion in South East Asia**, In Hondbook of Blockchain, Digital Finance, and Inclusion, Academic Press, Vol 2, 2018.
18. Kritika Law, **Impact of Perceived Security on Consumer Trust in Online Banking,** Auckland New Zealand, 2007.
19. Neittaanmaki Pekka, Lehto Martti, **Cyber Security: Analytics, Technology and Automation,** Switzerland: Springer international Publishing, 2015.
20. Nesselroade McArdle**, Longitudinal Data Analysis Using Structural Equation Models 1ed**, Washington USA: American Psychological Association, 2014, p 28.
21. Perry Hilton, Isabella Murray, Charlotte Brownlow**, SPSS Explained**, 2nd Edition, London, 2014.
22. Ramjee Prasad, Vandana Rohokale, **Cyber Security: The Lifeline of Information and Communication Technology**, published by springer, India, 2019.

23. Raphael Grevisse Yende, **Support de Cours de Sécurité Informatique et Crypto**, Congo Kinshasa, 2018.
24. Refalo pierre, **La Sécurité Numérique de L'entreprise l'effet papion du hacker,** Eyrolles, Paris, 2013.
25. Richard Clarkeand, Robert Knake, **Cyber War is the Next Threat to National Security and ways to Confront it**, harper colins Publishers, 10 east 53 rd Street, New York, 2012.
26. Santos, Cristiane Pizzutti**, Antecedents and consequences of consumer trust in the context of service recovery,** Brazilian Administration Review, Vol 5, N 3, 2008.
27. William Crumpler**, "The cybersecurity workforce gap in the commercial companies",** by the center for strategic and international studies, America, 2018.
28. William Leslie Dorotinsky, Joanna Alexandra Watkins, Cem Dener, **Financial Management Information Systems**, The world Bank, Copyright Clearance Center Inc, Columbia, Washington, 2011.

- **II. University Research:**

A) Doctoral Dissertations:

1. Ahmad Shammont, **Evaluating an Extended relationship Marketing Model for Arab Guests of Five star hotels**, PHD Thesis, school of Hospital, Tourism and Marketing, Victoria University-Melbourne, 2007.
2. Khalid Khalil, **"Cyber Security in Electronic Banking and its Impact Upon Electronic Banking",** Thesis is to Business Administration Department of IQRA National University, Peshawar, Khyber Pakhtunkhawa, Pakistan In Partial Fulfillment of the Requirements for the degree of Doctor of Philosophy in Management Sciences Business", 2021.
3. Van-Hoan Vu, **Infrastructure de gestion de la confiance sur internet**, thèse de doctorat, Ecole Nationale Supérieure des Mines de Saint-Etienne, Français, 2010.
4. Vincent Alimi, **Contributions au Déploiement des Services Mobiles et a L'analyse de la Sécurité des Transactions**, Thèse

présentée en vue de l'obtention du doctorat en informatique et applications, université de Caen – basse Normandie, 2012.

B) Master Messages :

1. Miska Laakkonen, **"Elements of Trust and Their Impact on Purchase Intention and Customer Loyalty of Online Service Users-Cyber Security Perspective",** Master's Thesis is to School of Science, Department of Computer Science, Aalto University, Finland, 2017.
2. Muamer Azizi, **"Pengaruh Persepsi Manfaat, Persepsi Kemudahan Penggunaan Dan Kemudahan, Kepercayaan Dan Persepsi Risiko Terhadap Minat Masyarakat Menggunakan Fasilitas Electronic Banking Bank Syariah Dengan Kepercayaan Sebagai Variabel Intervening, Studi Kasus Masyarakat Kecamatan Ungaran Timur Kabupaten Semarang"**, International Islamic University Malaysia, College of Islamic Economics and Business, Islamic Banking Institute, Master's Thesis Electronic Banking Services, Malaysia, 2018.
3. Younes Ait Mouhoub, Fatah Bouchebbah, **Proposition d'un modèle de confiance pour l'Internet des Objets**, Mémoire de master, Université A/Mira de Bejaia, Faculté des Sciences Exactes, Promotion 2015.

- **III. Scientific Articles:**

1. Ali Muhammad, Syed Ali Raza, Puah Chin Hong, Amin Hanudin, **How Perceived Risk, Benefit and Trust Determine User Fintech Adoption: a new Dimension for Islamic Finance**, Foresight, Vol 23, N 4, 2021.
2. Amin Shaqrah, Read Alqirem, Khaled Alomoush, **Affecting Factors of Knowledge Sharing on CRM: An Empirical Investigation Using Structural Equation Modeling**, World Journal of Social Sciences, Vol 01, N 01, 2011.
3. Amirhosein Mosavi, Assefa Melesse, Subodh Chandra Pal, **Flash Flood Susceptibility Modeling Using New Approaches of Hybrid**

and Ensemble Tree-Based Machine Learning Algorithms, Journal Remote Sens, Vol 12, N 3568, 2020.

4. Amiri, Hazarika, Deepti Dabas Hazari, **Investigating The Effect Of Trust In Accepting Electronic Services: A Case Of New Kabul Bank**, European Journal of Molecular & Clinical Medicine, University of Granada, Spain, Vol 7, N 6, 2020.
5. Amos Olushola Michael, **The Effect of Electronic Banking on Bank Performance in Nigeria, European Journal of Business and Management**, Vol 12, N 26, 2020.
6. Anthony Pugliese, Ronald Halse**, SysTrust and WebTrust Technology Assurance Opportunities,** CPA Journal, 2000.
7. Arya Himanshu**, E-Banking: The Emerging Trend**, International Journal of Trend in Scientific Research and Development IHTSRD, Vol 3, N 4, Jun 2019, P 452.
8. Ba Sulin, Pavlou Paul, **Evidence of Trust Building Technology in Electronic Markets: Price Premiums and Buyer Bahavoir. MIS Quality**, Vol 26, N 03, 2002.
9. Byrne k, **How do Consumers Evaluate Risk in Financial Products**, Journal of Finance Services Marketing, Vol 10, N 1, 2010.
10. Christine Ennew, Sekhon Harjit Singh, **Measuring Trust in Financial Services: The Trust Index**, Vol 17, N 2, 2007.
11. Chuang Limin, Kao Hsiao, Liu Chun, **The Adoption of Fintech Service: TAM Perspective.** International Journal of Management and Administrative Sciences, Vol 3, N 7, 2016.
12. David Gefen, **E-Commerce: The Rol of Familiarity and Trust OMEGA**, Vol 28, N 6, 2000.
13. Deepak Sideshmukh, Jagdip Singh, Barry Sabol, **Consumer Trust, Value, and Loyalty in Relational Exchanges**, Journal of Marketing, Vol 66, N 1, 2002.
14. Hamed Al nasrawi, Ali Al tameeni, **Thabit Thabit, Then Impact of Organizational Dogmatism in Reducing the Employees Internal Marketing**, Internasional Journal of Social Sciences Educational Studie, Vol 05, N 01, 2018.
15. Hamed Taherdoos**, Validity and Reliability of the Research Instrument, How to Test the Validation of a How to Test the**

Validation of a, International Journal of Academic Research in Management, Vol 5, N 3, 2016.

16. Hamid Mohamed Rashid, Sami Waqas, Sidek Mohamed, **Discriminant Validity Assessment: Use of Fornell Larcker Criterion Versus HTMT Criterion**, Journal of Physics: Conf Serie 890, 2017, p p 1-5.
17. Harrison Stewart, Jan Jurjens, **Data Security and Consumer Trust in FinTech Innovation in Germany, Information and Computer Security,** Vol 23, N 1, 2018.
18. Hernandez José Mauro, Mazzon José Afonso**, Adoption of Internet Banking: Proposition and Implementation of an Integrated Methodology Approach**, International Journal of Bank Marketing, Vol 25, N 2, 2007.
19. Hong Ilyoo, **Understanding the Consumers online marchant selection Process: The roles of Product Involvement, Perceived Risk, and Trust Expectation**, International Journal of Information Management, Vol 35, N 3, 2015.
20. Hu Zhongqing, Ding Shuai, Chen Luting, Yang Shanlin, **Adoption Intention of Fintech Services for Bank Users: An Empirical Examination with an Extended Technology Acceptance Model**, Symmetry, Vol 11, N 3, 2015.
21. Ibrahim Maimunatu, Umar Muazu, **"Security and Privacy Dimension as Predictor of Internet Banking E-Service Quality on Customer Trust"**, International Journal of Innovative Science and Research Technology, ISSN N 2456-2165, Vol 6, N 11, 2021.
22. Jorg Henseler, Christian Ringle, Marko Sarstedt, **A New Criterion for Assissing Discriminant Validity in Variance-based Structual Equation Modeling,** Journal if the Academy of Marketing Science, Vol 43, N 1, 2015.
23. Jorg Henseler, Sarstedt Marco, **Goodness of fit Indices for Partial Least Squares Path Modeling**, Computational Statistics, Vol 28, N 02, 2013.
24. Junger Moritz, Mark Mietzner, **Banking Goes Digital: The Adoption of FinTech Services by German Households**, Finance Research Letters, 2020.
25. Ken Wong Kay Kwong, **Mediation Analysis, Categorical Moderation Analysis, and Higher Order Constructs Modeling**

in Partial Least Squares Structual Equation Modeling (PLS-SEM): A B2B Example Using Smart PLS, Marketing Bulletin, Vol 26, N 1, 2016.

26. Lydiah Wambugu، **Impact of Internal Marketing on Service Quality and Customers "Satisfaction (A Case Study of Equity Bank, Kengeleni Branch)"** ، Research Journal of Finance and Accounting، vol 6, No 19, 2015.

27. Lynne Richardson, John Swan, Michael Bowers**, Customer Trust in The Salesperson: An Integrative Review and a Meta-Analysis of The Empirical Literature**, Journal of Business Research, Vol 44, 1999.

28. Mahdi Nasr Esfahani, **"E-Bank Services: Analyzing the Effect of E-Bank Service on E-Trust with E-Security Approach "**, European Research Studies Journal, Department of the University of Malta, Vol 202, N 01, 2019.

29. Margaret Tan, Thompson Teo, **Factors Influencing the Adoption of Internet Banking**, Journal of the AIS, Vol 1, N 5, 2000.

30. Marko Sarstedt, Christian Ringle, Joseph Franklin Hair, **Partial Least Squares Strudtural Equation Modeling**, Journals Industrial Management Data Systems, Vol 123, N 12, 2021.

31. Martin Wetzels, Gaby Schroder Odekerken, Claudia Oppen, **Using PLS Phath Modeling for Assessing Hierarchical Construct Models: Guidelines and Empirical Illustration MIS Quarterly**, Vol 33, N 1, 2009.

32. Maruf Gbadebo Salimon, Rushami Zien Yusoff, Sany Sanuri Mohd Mokhtar,**" The Impact of Perceived Security on E-Trust, E-Satisfaction and Adoption of Electronic Banking in Nigeria: A Conceptual Review",** IOSR Journal of Business and Management (IOSR-JBM), University Utara Malaysia, Vol 1, N 1, 2015.

33. Mbama Cajetan Ikechukwu, Ezepue Patrick Oseloka, Alboul Lyuba, Beer Martin**, Digital Banking, Customer Experience and Financial Performance, Journal of Research in Interactive Marketing**, Vol 12, N 4, 2018.

34. Meryl Nangin Astin, Razita Gloria Barus Irma, Wahyoedi Soegeng, **The Effects of Perceived Ease of Use, Security, and Promotion on Trust and Its Implications on Fintech Adoption**, Journal of Consumer Sciences, Vol 5, N 2, 2020.

35. Mircea Fuciu, **The Consumer Confidence Report- A Tool For Developing Marketing Strategies Designed For The Online Environment**, Annals Univeresitatis Apulensis Series Oeconomica, Vol 19, N 2, 2017.

36. Mohammed Al-Sharafi, Ruzaini Arsha, Emad Abu-Shanab, Nabil Elayah, **"The Effect of Security and Privacy Perception on Customers Trust to Accept Internet Banking Services: An Extension of TAM"**, Journal of Engineering and Applied Sciences, Britain, Vol 11, N 3, 2016.

37. Qais Hamouri, Tahaer Majali, Damaithan Almajali, Abdalrazzaq Aloqool, Jassim Ahmad Al-Gasawneh, **"Explore the Relationship between Security Mechanisms and Trust in E-Banking: A Systematic Review"**, Annals of R.S.C.B, ISSN: 1583-6258, Vol 25, N 6, 2021.

38. Raija Jarvinen, **Consumer Trust in Banking Relationships in Europe**, International Journal of Bank Marketing, Vol 32, N 6, 2014.

39. Rasoolimanesh Seyyed, **Discriminant Validity Assessment in PLS-SEM: A ComprehensiveComposite-Based Approach**, Data Analysis Perspectives Journal, Vol 3, N 2, 2022.

40. Roberts Lombard, Estelle Tonder, Theuns Pelser, Johannes Prinsloo**, The Relationship Between Key Variables and Customer Loyalty Within the Independent Financial Advisor Environment**, The Retail and Marketing Review, Vol 10, N 01, 2014.

41. Robert Morgan, Shelby Hunt, **The Commitment Trust Theory of Relationship Marketing**, Journal of Marketing, Published By: Sage Publication, INC, Vol 58, N 3, 2015.

42. Roland Kantsperger, Kunz Werner, **Consumer Trust in Service companies: a Multiple Mediating analysis**, Managing Service Guality, Vol 20, N 01, 2010.

43. Peng Lee Moghavemi, **The Dimension of Service Quality and Its Impact on Customer Satisfaction, Trust, and Loyalty: A Case of Malaysian Bank,** Asian Journal of Business and Accounying, Vol 8, N 2, 2015.

44. Rotter Julian, **A New Scale For the Measurement of Interpersonal Trust**, Journal of Personality, Vol 35, N 4, December 1967.
45. Roy Sanjit, **Dimensions of True and Trustworthiness in Retail Banking: Evidence from India**, Marketing Management Journal, Vol 21, N 1, 2011.
46. Salo Jari, Karjaluoto Heikki, **a Conceptual Model of Trust in the Online Environment, Online Information Review**, Vol 31, N 5, 2007.
47. Sandra Streukens, Sara Leroi Werelds, **Bootstrapping and PLS-SEM / A step by step guide to get more out of your Bootstrap Results**, Europen Management Journal, Vol 34, N 6, 2016.
48. Sarstedt Marko, Hair Joe, **Christian Ringle, Partial Least Structural Equation** Modeling, Sage Publications Inc, 2nd Editio, Thousand Oaks, 2017.

- **IV. Scientific Demonstrations:**

International Forums:

1. Musbah abdulkarim, Musbah Ataya, Musab Ali, **"Acceptance of Website Security on E-banking",** IEEE 10th Control and system Graduate Research Colloquium (ICSGRC), Shah Alam, Malaysia, 2-3 August 2019.

- **V. Websites:**

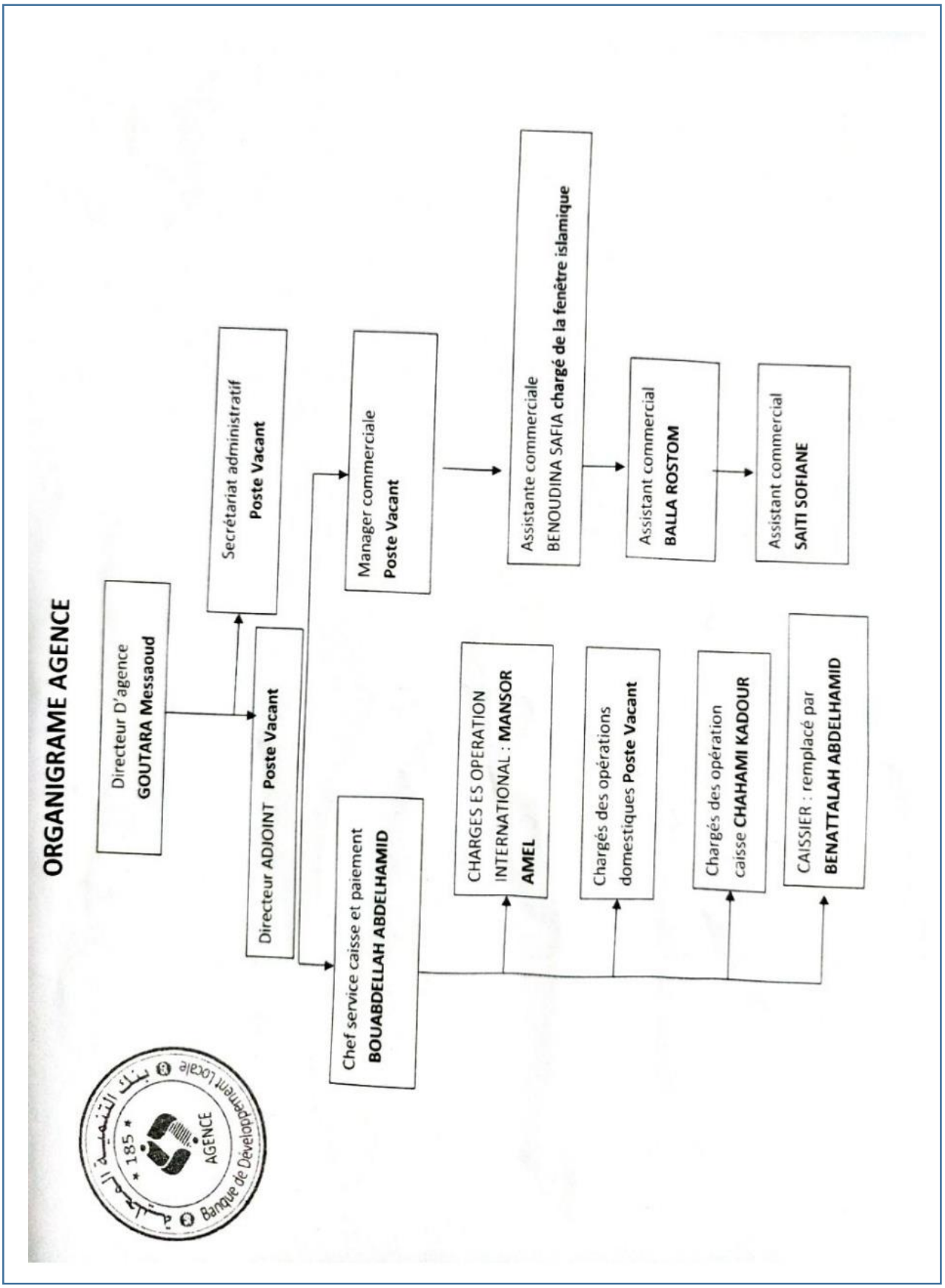
1. https://aaltodoc.aalto.fi/bitstream/hadle/123456789/29197.
2. https://annalsofrscb.ro.
3. https://ar.wikipedia.org.
4. https://blog.araboost.com/influencers-marketing-stratistics.
5. https://cbi.iq/static/uploads/up/file-152377270192790.
6. https://code.google.com/p/google-security-research/issues/list.
7. https://cutt.us/U3gSP.
8. https://doi.org/10.31559/GJEB2020.8.3.3.
9. https://doi.org/104135/9781452231327.
10. https://doi.org/10.2307/1252308.
11. https://doi:10.1016/S0305-0483(00)00021-9.

12. https://doi.org/10.2307/4132332.
13. https://doi.org/10.1111/j.1467-494.1967.tb01454.x.
14. https://doi:10.29302/oeconomica.2017.19.2.3.
15. https://doi:10.1108/09604521011011603.
16. https://doi.org/10.51173/jt.v5i1.1218.
17. https://doi.org/10.1590/s1807-76922008000300005.
18. https://doi:10.31142/ijtsrd23689.
19. https://doi.org/10.1016/j.ijinfomgt.2015.01.003.
20. https://doi.org/10.3390/sym11030340.
21. https://doi.org/10.1108/JRIM-01-2018-0026.
22. https://doi.org/10.1108/ICS-06-2018-0039.
23. https://doi.org/10.1016/j.frl.2020.08.008.
24. https://doi.org/10.29244/jcs.5.2.124-138.
25. https://doi.org/10.1108/FS-09-2020-0095.
26. https://dx.doi.org/10.21608/acj.2021.204475.
27. http://ecommercetechnology.org/data/88.htm.
28. http://faculty.ksu.edu.sa/mas/published%20papers/EC%20STRATEGY.pdfconsulté12/08/20.
29. https://hal.science/cel-01965300/document.
30. https://ieeemy.org/section/2019-10th-ieee-control-and-system-graduate-research-colloquium-icsgrc-2019.
31. https://prr.hec.gov.pk/jspui/bitstream/23456789/17574/1/khalid%khalil1.
32. https://www.nsa.gov.(US National Security Agency).
33. https://seaech.mandumah.com/Record/630109.
34. https://shodhganga.inflibnet.ac.in/bitstream/10603/175638/4/13-chapter-5.pdf.
35. https://t8t.in/%D8%AA%D9%82%D9%86%D9%8A%D8%A9.
36. https://www.frameip.com/firewall.
37. https://www.sans.org/about.
38. https://www.arabic.cnn.com/business/six-steps-keep-your-clients.
39. https://www.nysscpa.org/cpajournal/2000/1100/features/f112800
40. https://www.arabiya.net.
41. https://www.websiterating.com.
42. https://www.addustour.com.
43. https://www.researchgate.net/publication/285769675.
44. https://www.emeraldinsigh.com/1468-4527.htm.

45. https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CPDP%202015%20-%20KORFF %20Handout.pdf.
46. https://www.rattibha.com.
47. https://www.rmg-sa.com
48. http://www.itu.int.
49. https://www.arabia2.com/vb.
50. https://www.commerce.gov.dz.
51. https://www.bdl.dz.
52. https://www.ijisrt.com.
53. https://www.noor-book.com.
54. htps://www.bbc.com/Arabic/world-49166226.

قائمة الملاحق

الملحق رقم (01): الهيكل التنظيمي لبنك التنمية المحلية BDL بولاية غرداية



الملحق رقم (02): الاستبيان

وزارة التعليم العالي والبحث العلمي

ميدان: علوم اقتصادية والتسيير وعلوم تجارية

شعبة: علوم تجارية، تخصص تسويق الخدمات

أخي الفاضل ....أختي الفاضلة:

السلام عليكم...

يسرنا أن نضع بين أيديكم هذا الاستبيان الذي تم تصميمه لجمع المعلومات اللازمة للدراسة التي نقوم بإعدادها استكمالا لنيل شهادة دكتوراه تخصص تسويق الخدمات من خلال إعداد أطروحة بعنوان: "**مساهمة الأمن السيبراني للبيانات في تعزيز ثقة العملاء نحو الخدمات الإلكترونية المصرفية (دراسة ميدانية لدى عينة بنك التنمية المحلية بمدينة غرداية)**".

نأمل منكم التكرم بالإجابة على أسئلة الاستبيان بدقة، بحيث أن صحة النتائج تعتمد بدرجة كبيرة على صحة إجاباتكم، فرأيكم عامل أساسي من عوامل الوصول إلى نتائج دقيقة.

ونحيطكم علما أن جميع إجاباتكم لن تستخدم إلا لأغراض البحث العلمي فقط، مع ضمان السرية التامة للإجابات.

تفضلوا بقبول فائق التقدير والاحترام

يمكنكم الحصول على نسخة من ملخص نتائج البحث بالاتصال عبر البريد الإلكتروني التالي:

Souag.abdelkader@univ-ghardaia.dz

من إعداد الطالب: عبد القادر صواق.

تحت إشراف:

الدكتور: بومدين بوداود.

الأستاذ الدكتور: عبد اللطيف أولاد حيمودة.

رقم الاستبيان: ☐

أولا: البيانات الخاصة بالمستجيب:

1. **الجنس:** ذكر ☐ أنثى ☐

2. **العمر:** 26 سنة فما أقل ☐ من 26-35 ☐ 36-45 ☐ أكثر من 46 ☐

3. **المستوى التعليمي:** ثانوي فما أقل ☐ باكالوريا ☐ جامعي ☐ دراسات عليا ☐

4. **المهنة:** موظف بالقطاع العام ☐ عامل بالقطاع الخاص ☐ أخرى أذكرها من فضلك ☐

5. **الدخل:** أقل من 18000دج ☐ من 18000-45000دج ☐ من 45000-90000دج ☐ أكثر من 90000دج ☐

6. **مدة التعامل مع البنك:** أقل من سنة ☐ من 1 إلى 5 ☐ من 6-10 ☐ أكثر من 11 ☐

ثانيا: الرجاء قراءة العبارات الآتية ووضع علامة (X) في الحقل المناسب.

المحور الأول: الأمن السيبراني للبيانات (Data Cyber Security)

I	سرية البيانات (Confidentiality):	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
1)	يحرص البنك على إعطائي رقما سريا خاصا للبطاقة الإلكترونية منذ يوم التسليم.					
2)	يتأكد البنك من هويتي وصلاحية دخولي في كل معاملة إلكترونية أقوم بها.					
3)	الرقم السري لبطاقتي الإلكترونية يصعُب قرصنتها.					
4)	يُتيح لي البنك إمكانية تغيير الرقم السري عند الحاجة.					
5)	ليس بإمكان أي شخص الولوج إلى حسابي الإلكتروني قصد الاطلاع على بياناتي ومعلوماتي.					
II	التوافر والديمومة (Availability):	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
1)	الخدمات الإلكترونية للبنك متاحة باستمرار لمدة 24 ساعة في اليوم وخلال كل أيام الأسبوع.					
2)	خدمات المصرف متاحة في كل مكان.					

3)	يتيح البنك امكانية الولوج الإلكتروني إلى بياناتي لتدقيقها في أي وقت.					
4)	يوفر البنك مجموعة متنوعة من وسائل الاتصال به بصفة دائمة مثلا: Internet-Mobile-Fax-Mail-SMS					
5)	من خلال تعاملاتي السابقة بالبطاقة الإلكترونية، لم يسبق لي وأن صادفت عطل أو خلل في الجهاز ما أدى إلى انقطاع الخدمة.					

III	تتبع الأثر (Traceability):	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
1)	يقوم البنك بتوثيق وتسجيل جميع تعاملاتي الإلكترونية بصفة تلقائية.					
2)	يمكنني مراجعة وتقفي جميع مسارات المعاملات الإلكترونية التي قمت بها ومعرفة تاريخها وتوقيتها.					
3)	يشعرني البنك بالعمليات التي أقوم بها، كسحب الرصيد، التحويلات، الخصم، الدفع، وغير ذلك.					
4)	تقوم آلة الموزع الآلي بسحب بطاقتي الإلكترونية تلقائيا عند استعمالها بشكل خاطئ باستمرار.					
5)	يتم تجميد حسابي في حال فقدان البطاقة.					
IV	التكنولوجيا المستخدمة (Technology Used):	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
1)	يقدم البنك خدماته بمعدات وأجهزة تقنية متطورة.					
2)	أنظمة البنك وأجهزته تعمل بدقة دون أي خلل.					
3)	نسبة الأخطاء في نظام المعلومات الخاص بمعاملاتي الإلكترونية مع البنك معدومة بشكل عام.					
4)	البنك يستخدم تكنولوجيا بمعايير دولية في إدارة وحماية شبكات الاتصال والبطاقات الإلكترونية.					
5)	عمليات بطاقة الدفع أو السحب الإلكترونية تتم بسرعة عالية وهي توفر لي الجهد والوقت.					

V	احترام الخصوصية (Privacy):	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
1)	أثناء تعاملي مع البنك يطلب مني الإدلاء فقط بالمعلومات التي أقبل الإفصاح عنها.					
2)	بياناتي الشخصية محفوظة في بطاقة الدفع الإلكترونية وسليمة المحتوى ويمكنني تعديلها في حال احتجت ذلك.					
3)	يحرص البنك على عدم نشر أو بَث بياناتي الشخصية.					
4)	البنك يحترم خصوصية بياناتي الشخصية ولا يشاركها مع أطراف أخرى.					
5)	البنك يحمي ويحافظ على بياناتي الشخصية والمعلومات التي جمعها عني ولا أتوقع يوما أن يُتاجر بها.					

المحور الثاني: (الثقة Confidence)

VI	البعد المعرفي (Cognitive Dimension)	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
1)	أثق بجوانب الأمان المتعلقة باستخدام الخدمات الإلكترونية المصرفية.					
2)	البنك الذي أتعامل معه لديه القدرة والكفاءة في تقديم خدماته المصرفية الإلكترونية التي أحتاجها.					
3)	البنك لديه خبرة كافية لأداء الخدمات الإلكترونية بكل فعالية والتزام.					
4)	سياسة البنك وقوانينه الموجودة حاليا توفر لي الحماية عند استخدام الخدمات الإلكترونية المصرفية.					
5)	البنك يتعامل بكل مصداقية وإخلاص.					
VII	البعد العاطفي (Emotional Dimension)	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة

1)	أشعر بالأمان في اعتمادي التعامل إلكترونيا مع البنك.					
2)	أعتقد أن البنك يريد لي الأفضل بتعاملاته الإلكترونية.					
3)	البنك يأخذ بعين الاعتبار مصلحتي واهتمامي من خلال نفعي بالخدمات الإلكترونية المصرفية بأفضل طريقة.					
4)	أرى أن البنك يبذل العناية والجهد اللازم من أجل حماية بياناتي الشخصية.					
5)	يستجيب البنك بسرعة لحل أي مشكلة تصادفني تتعلق بسلامة وأمن البطاقة الإلكترونية.					

المحور الثالث: الخدمات الإلكترونية المصرفية (Electronic Banking Services)

VIII	(الخدمات الإلكترونية المصرفية)	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
1)	الخدمات المصرفية الإلكترونية أفضل بكثير من الخدمات المصرفية التقليدية وهي تلبي متطلباتي.					
2)	تشجعني السياسة الأمنية للبنك الخاصة باستعمال البطاقات الإلكترونية على استمرارية التعامل معه.					
3)	درجة اهتمام البنك بأمن بياناتي الشخصية المتعلقة بالخدمات الإلكترونية المصرفية تجعلني في ثقة وارتياح.					
4)	البنك يحمي ويؤمّن بياناتي الشخصية أثناء استخدام الخدمات الإلكترونية المصرفية أكثر مما توقعت.					
5)	سوف أوصي الآخرين باستخدام الخدمات الإلكترونية المصرفية.					

الملحق رقم (03): قائمة الأساتذة المحكمين للاستبيان

الرقم	الأستاذ	الجامعة
01	أ.د سليمان صادق درمان	رئيس قسم إدارة الأعمال بكلية الإدارة والاقتصاد جامعة دهوك بدولة العراق Drman1957@yahoo.com
02	أ.د هواري معراج	جامعة غرداية
03	د. محجوبي محمد الأخضر	جامعة غرداية
04	د. محمد البشير ثامر	جامعة غرداية
05	د. كمال قريني	جامعة معسكر

الملحق رقم (04): قائمة أسماء المهنيين محكمي الاستبيان

الرقم	الاسم واللقب	المنصب	اسم المؤسسة التي يشتغل بها
01	محمد فسيو	المنسق الجهوي للدفع الإلكتروني	بنك التنمية المحلية غرداية
02	فريد عايد	مراقب عملياتي	بنك التنمية المحلية غرداية
03	أمين رحماني	ضابط شرطة رئيسي	رئيس فرقة مكافحة الجريمة المعلوماتية بأمن ولاية غرداية
04	علي دامة	ضابط شرطة رئيسي	المصلحة الولائية للوسائل التقنية بأمن ولاية غرداية
05	أ. بن يمينة مريم	محامية معتمدة لدى المحكمة العليا مجلس الدولة	محامية بولاية غرداية