وزارة التعليم العالي والبحث العلمي
جامعة الشهيد الشيخ العربي التبسي –تبسة–
كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير

قسم العلوم التجارية

الرقم التسلسلي: ...../ 2026

مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي (ل م د)

فرع: علوم تجارية

التخصص: تسويق الخدمات

المذكرة موسومة بـ:

فعالية الأمن السيبراني في حماية بيانات العملاء
دراسة حالة مؤسسة اتصالات الجزائر –تبسة–

من إعداد الطالبين:
- **حمزة جابري**
- **محمد شامخ زرقان**

تحت إشراف الأستاذة:
- **بسمة عولمي**

أعضاء لجنة المناقشة المتكونة من الأساتذة:

اسم ولقب الأستاذ	الرتبة العلمية	جامعة الانتساب	الصفة
أسمهان بوعشة	أستاذ محاضر ب	جامعة الشهيد الشيخ العربي التبسي– تبسة	رئيسا
بسمة عولمي	أستاذ	جامعة الشهيد الشيخ العربي التبسي– تبسة	مشرفا ومقررا
عبدد الرحمان رايس	أستاذ محاضر أ	جامعة الشهيد الشيخ العربي التبسي– تبسة	مناقشا

السنة الجامعية: 2025 - 2026


بسم الله الرحمن الرحيم

شكر وعرفان

الحمد لله تعالى الذي وفقنا لإتمام هذا العمل، وأعاننا بنعمه التي لا تُعدّ ولا تُحصى، فله الحمد أولًا وآخرًا على نعمة العلم والمعرفة، التي جعلها سبيلًا للرقي والنجاح، وطريقًا نحو بناء المستقبل وخدمة المجتمع.

ويسرّنا في هذا المقام أن نتقدّم بخالص عبارات الشكر والعرفان والتقدير إلى جميع أساتذتنا الأفاضل، الذين لم يبخلوا علينا بعلمهم وتوجيهاتهم ونصائحهم القيّمة، وكان لهم الفضل الكبير فيما وصلنا إليه، فجزاهم الله عنا خير الجزاء، وجعل ما قدموه في ميزان حسناتهم.

كما نتوجّه بالشكر الجزيل إلى كل من ساهم من قريب أو بعيد في إنجاز هذه الدراسة، سواء بالدعم أو التوجيه أو تقديم المعلومات والتسهيلات التي ساعدتنا في إتمام هذا العمل في أحسن الظروف.

ولا يفوتنا أن نعبر عن امتناننا لكل من زرع فينا روح التفاؤل والعزيمة، وساندنا خلال مسيرتنا الدراسية، فله منا كل الاحترام والتقدير والعرفان.

وفي الأخير نسأل الله تعالى أن يبارك في جهود الجميع، وأن يوفقنا وإياهم لما يحب ويرضى، وأن يجعل هذا العمل خالصًا لوجهه الكريم ونافعًا لكل طالب علم.

وصلى الله وسلم على سيدنا مُحَمَّد وعلى آله وصحبه أجمعين، والحمد لله رب العالمين

إهداء

الى كل من كلل العرق جبينه ومن علمني ان النجاح لا يأتي الا بالصبر والإصرار الى النور الذي انار ..... دربي والسراج الذي لاينطفئ نوره بقلبي ابدا

.... الى من بذل الغالي والنفيس واستمديت منه قوتي واعتزازي بذاتي

.....ابي

..... الى من جعل الجنة تحت اقدامها وسهلت بي الشدائد بدعائها

.. امي

الى ضلعي الثابت و امان ايامي

..... الى من شددت عضدي بهم فكانوا ينابيع ارتوي منها الى خيرة ايامي وصفوتها

...اختي... اخي

للاصدقاء الاوفياء ورفقاء السنين لاصحاب الشدائد والازمات... لكل من كان عونا في هذا الطريق

الفهارس

فهرس المحتويات

شكر وعرفان

إهداء

الفهارس

b فهرس الجداول

فهرس الأشكال

المقدمة العامة

المقدمة العامة

يشهد العالم المعاصر تحولات رقمية متسارعة مست مختلف القطاعات الاقتصادية والخدمية، حيث أصبحت المؤسسات تعتمد بصورة متزايدة على الأنظمة الرقمية والتطبيقات الإلكترونية في إدارة أعمالها وتقديم خدماتها للعملاء، الأمر الذي أسهم في تحسين جودة الخدمات وتسريع المعاملات وتعزيز التواصل مع الزبائن. غير أن هذا التطور التكنولوجي صاحبه تزايد ملحوظ في التهديدات الإلكترونية والهجمات السيبرانية التي تستهدف الأنظمة المعلوماتية وقواعد البيانات، خاصة تلك المتعلقة بالمعطيات الشخصية والمالية للعملاء، مما جعل قضية حماية المعلومات من أهم التحديات التي تواجه المؤسسات الحديثة. وفي ظل هذا الواقع الرقمي الجديد، برز مفهوم الأمن السيبراني باعتباره أحد الركائز الأساسية لضمان استمرارية النشاط المؤسسي والحفاظ على سرية البيانات وسلامتها، إضافة إلى تعزيز الثقة في البيئة الرقمية والمعاملات الإلكترونية، خاصة داخل المؤسسات الخدمية التي تعتمد بشكل مباشر على بيانات العملاء وتفاعلاتهم الإلكترونية.

ويُعد الأمن السيبراني منظومة متكاملة من السياسات والإجراءات والتقنيات التي تهدف إلى حماية الأنظمة والشبكات والبرمجيات والبيانات من الاختراق أو التلاعب أو التسريب، من خلال استخدام مجموعة من الآليات التقنية والتنظيمية التي تعتمدها المؤسسات الخدمية لضمان أمن معلوماتها الرقمية. وتشمل هذه الآليات جدران الحماية الإلكترونية، وتقنيات التشفير، وأنظمة كشف التسلل، والمصادقة متعددة العوامل، والنسخ الاحتياطي للبيانات، بالإضافة إلى السياسات التنظيمية المتعلقة بإدارة كلمات المرور، وتوعية العاملين، ومراقبة استخدام الأنظمة الرقمية، ووضع خطط للاستجابة للحوادث السيبرانية. وقد أصبحت فعالية هذه الآليات معيارًا أساسيًا في تقييم قدرة المؤسسات على حماية بيانات عملائها من المخاطر الرقمية المختلفة، خصوصًا مع تزايد اعتماد العملاء على الخدمات الإلكترونية والتطبيقات الذكية. كما أن توفير بيئة رقمية آمنة يسهم بصورة مباشرة في تعزيز الثقة التسويقية لدى العملاء، إذ يشعر الزبون بدرجة أكبر من الاطمئنان عند التعامل مع مؤسسة تضمن سرية. معلوماته وتحافظ على خصوصيته، وهو ما ينعكس إيجابًا على ولائه واستمرارية تعامله مع المؤسسة، باعتبار أن الثقة الرقمية أصبحت عنصرًا حاسمًا في بناء العلاقات التسويقية الحديثة. وتشير العديد من الدراسات إلى أن تطبيق آليات الأمن السيبراني بفعالية يساهم في حماية السمعة المؤسسية وتقليل الخسائر الناتجة عن الهجمات الإلكترونية وتعزيز القدرة التنافسية للمؤسسات الخدمية.

وفي هذا السياق، أولت الدولة اهتمامًا متزايدًا بمجال الأمن السيبراني وحماية البيانات الرقمية، خاصة في ظل توجهها نحو الرقمنة وتوسيع استخدام الخدمات الإلكترونية في مختلف القطاعات الإدارية

والاقتصادية والخدمية. وقد تجسد هذا الاهتمام من خلال سن العديد من التشريعات والقوانين المتعلقة بحماية المعطيات ذات الطابع الشخصي وتعزيز أمن الأنظمة المعلوماتية، إضافة إلى إنشاء هيئات ومؤسسات متخصصة في متابعة التهديدات السيبرانية وتأمين البنية التحتية الرقمية الوطنية. كما عملت الجزائر على تطوير استراتيجيات وطنية تهدف إلى تعزيز المرونة السيبرانية وحماية المؤسسات والمواطنين من المخاطر الإلكترونية، إلى جانب تنظيم دورات تكوينية وبرامج توعوية لنشر ثقافة الأمن الرقمي داخل المؤسسات والمجتمع. وتبرز أهمية هذا الموضوع في كونه يرتبط بحماية البيانات الحساسة وضمان استقرار المعاملات الرقمية، فضلًا عن دوره في تعزيز ثقة العملاء في الخدمات الإلكترونية التي تقدمها المؤسسات الخدمية الجزائرية، الأمر الذي ينعكس على تحسين الأداء التسويقي وزيادة رضا العملاء وولائهم. كما أن دراسة فعالية آليات الأمن السيبراني أصبحت ضرورة علمية وعملية لفهم مدى قدرة المؤسسات الجزائرية على مواكبة التحولات الرقمية والتصدي للتحديات السيبرانية المتزايدة، خاصة مع تنامي الاعتماد على الاقتصاد الرقمي والتجارة الإلكترونية والخدمات الذكية.

تقتضي الدراسة العلمية الرصينة لأي ظاهرة تسويقية وتكنولوجية معقدة، بناء هيكل منهجي يحدد مسارات البحث ويضبط أدوات القياس. يمثل هذا الإطار البوصلة التي توجه جهد الباحث نحو اختبار فروضه ميدانيا، عبر جمع البيانات، معالجتها إحصائيا، واستخلاص الدلالات التي تربط بين متغيري الأمن السيبراني وحماية بيانات العملاء.

أولا: الإشكالية

أفرزت التحولات الرقمية العميقة واقعا تشغيليا جديدا تعتمد فيه المؤسسات الخدمية بشكل كلي على تجميع وتحليل البصمة الرقمية لعملائها بغرض تخصيص العروض وبناء الميزة التنافسية. غير أن هذا الاستغلال المكثف لقواعد البيانات ألقى بهذه الكيانات في بيئة افتراضية شديدة الهشاشة، حيث تتصاعد التهديدات السيبرانية المتمثلة في الاختراقات وبرمجيات الفدية التي تستهدف السجلات الشخصية والائتمانية للمستهلكين. يولد هذا الانكشاف قلقا رقميا لدى العميل، مما يجعل من تبني تدابير حماية صارمة ضرورة حتمية ليس فقط لدرء المخاطر التقنية، بل لضمان استدامة العلاقة التسويقية وتكريس الثقة. بناء على هذا الطرح التحليلي، تتبلور معالم الإشكالية المركزية لهذه الدراسة في التساؤل الجوهري التالي : **ما مدى فعالية آليات الأمن السيبراني في حماية بيانات العملاء وتعزيز ثقتهم التسويقية لاسيما المؤسسات الخدمية الجزائرية؟**

تتفرع عن هذه الإشكالية المركزية مجموعة من التساؤلات الفرعية التي توجه مسار التحليل الميداني:

1. ما هو مستوى تطبيق المؤسسة الخدمية محل الدراسة للآليات التقنية والتنظيمية للأمن السيبراني؟
2. ما هو مستوى إدراك العملاء لفعالية الإجراءات الأمنية المتخذة لحماية خصوصية بياناتهم؟
3. هل توجد علاقة ذات دلالة إحصائية بين صرامة الأمن السيبراني ومستويات الثقة والولاء التسويقي لدى عملاء المؤسسة؟

ثانيا: فرضيات الدراسة

تمثل الفرضيات إجابات استباقية ومؤقتة للتساؤلات المطروحة، تتم صياغتها استنادا إلى التراكم المعرفي للفصول النظرية، وتخضع لالختبار الميداني لإثبات صحتها أو دحضها.

الفرضية العامة :توجد فعالية ذات دلالة إحصائية لآليات الأمن السيبراني المطبقة في حماية بيانات العملاء، مما ينعكس إيجابا على تعزيز الموثوقية الرقمية للمؤسسة الخدمية.

الفرضيات الجزئية:

1. توجد علاقة ارتباطية موجبة وذات دلالة إحصائية بين الآليات التقنية والتنظيمية للأمن السيبراني وبين ضمان مبادئ السرية والسلامة لبيانات العملاء.
2. يساهم الإدراك الإيجابي للعميل لفعالية الأمن السيبراني في تخفيض مستوى القلق الرقمي لديه.
3. توجد علاقة تأثير ذات دلالة إحصائية بين حماية بيانات العملاء سيبرانيا وبين تحقيق الميزة التنافسية وبناء الولاء التسويقي.

ثالثا: أسباب اختيار الموضوع

1. الأسباب الذاتية:

– الاهتمام المتزايد بموضوع الأمن السيبراني ودوره في حماية المعلومات الحساسة داخل المؤسسات الخدمية .

– الرغبة في فهم آليات حماية بيانات العملاء في ظل التحول الرقمي والتطور التكنولوجي .

– الميل إلى دراسة القضايا الحديثة المرتبطة بالتكنولوجيا وإدارة البيانات وتأثيرها على ثقة العملاء .

2. الأسباب الموضوعية:

– تزايد الهجمات والتهديدات الإلكترونية التي تستهدف المؤسسات الحافظة لبيانات العملاء.

– الأهمية الكبيرة لحماية البيانات الشخصية في قطاع الاتصالات باعتباره من أكثر القطاعات اعتماداً على الأنظمة الرقمية .

– الحاجة إلى تقييم فعالية إجراءات الأمن السيبراني المطبقة داخل مؤسسة اتصالات الجزائر ومدى مساهمتها في الحد من المخاطر السيبرانية .

– مساهمة الدراسة في إبراز العلاقة بين الأمن السيبراني وحماية خصوصية العملاء وتعزيز الثقة المؤسسية.

– حداثة الموضوع وأهميته العلمية والعملية في ظل التحول الرقمي المتسارع.

رابعا : أهداف الدراسة

– توضيح المفاهيم الأساسية المرتبطة بالأمن السيبراني وحماية البيانات .

– تحديد أهم التهديدات السيبرانية التي قد تستهدف بيانات العملاء في قطاع الاتصالات .

– التعرف على السياسات والإجراءات والتقنيات الأمنية المعتمدة في مؤسسة اتصالات الجزائر لحماية البيانات .

– تقييم مدى فعالية نظم الأمن السيبراني في تقليل مخاطر الاختراق والتسرب المعلوماتي .

– دراسة أثر الأمن السيبراني في تعزيز ثقة العملاء وحماية خصوصيتهم .

– تقديم توصيات عملية لتحسين مستوى الأمن السيبراني وحماية بيانات العملاء.

خامسا: أهمية الدراسة

– مساعدة مؤسسة اتصالات الجزائر على تشخيص مستوى فعالية إجراءات الأمن السيبراني المعتمدة لديها.

– المساهمة في اقتراح حلول وتوصيات لتعزيز حماية بيانات العملاء والحد من التهديدات الإلكترونية.

– تعزيز ثقة العملاء من خلال تحسين مستويات الخصوصية والأمن المعلوماتي .

– إثراء الأدبيات في مجال الأمن السيبراني وحماية البيانات، خاصة في قطاع الاتصالات .

– تقديم إطار نظري يوضح العلاقة بين فعالية الأمن السيبراني وحماية بيانات العملاء .

– دعم الدراسات الأكاديمية التي تتناول المخاطر الرقمية وإدارة أمن المعلومات.

سادسا : منهجية البحث

1. **المنهج المتبع** : لإنجاز هذه الدراسة والإحاطة بمختلف جوانبها، تم الاعتماد على المنهج الوصفي التحليلي الذي يصف الظاهرة المدروسة كميا وكيفيا. يتيح هذا المنهج تفكيك بنية الأمن السيبراني داخل المؤسسة الخدمية، ورصد انعكاساته على السلوك الاستهلاكي من خلال استخراج المتوسطات والانحرافات المعيارية التي تفسر طبيعة العلاقة بين المتغير المستقل (الأمن السيبراني) والمتغير التابع (حماية البيانات وثقة العميل). وتم تدعيم هذا المسار بالمنهج الارتباطي لقياس قوة واتجاه العلاقة بين هذه المتغيرات.

2. **مجتمع وعينة البحث** : يتكون مجتمع الدراسة من كافة عملاء المؤسسة الخدمية الجزائرية (يتم تحديد اسم المؤسسة كالبريد أو بنك معين لاحقا بناء على مكان التدريب). نظرا لاستحالة حصر جميع المفردات ومسحها بالكامل لاعتبارات الوقت والجهد، تم اللجوء إلى اختيار عينة ممثلة. اعتمدنا في هذه الدراسة على العينة العشوائية البسيطة التي تمنح كل فرد من أفراد المجتمع نفس فرصة الدخول في العينة دون استثناء. لتحديد الحجم الأمثل والمقبول إحصائيا الذي يقلل من نسبة الانحراف، تم الاستناد إلى معادلة ريتشارد جيجر (Richard Geiger) لضمان تمثيل دقيق يحقق نسبة خطأ ال تتجاوز 5% وبدرجة ثقة تبلغ 95.%

3. **مجالات الدراسة** :

المجال المكاني: اقتصرت الدراسة الميدانية على إحدى المؤسسات الخدمية الفاعلة في الاقتصاد الجزائري (تحدد المؤسسة لاحقا)

المجال الزماني: تمتد فترة الدراسة الميدانية وتوزيع الاستبيان واسترجاعه وتحليل بياناته خلال السداسي الثاني من الموسم الجامعي الحالي .المجال البشري: استهدفت الدراسة شريحة العملاء الذين يمتلكون تعاملات رقمية مباشرة مع المؤسسة المبحوثة ويشاركون بياناتهم عبر منصاتها.

4. **أدوات جمع البيانات:** بناء على طبيعة المنهج المعتمد، تم تصميم "الاستبيان" كأداة رئيسية لجمع البيانات الأولية من المبحوثين. تم بناء الاستبيان بالاعتماد على التراث النظري والدراسات السابقة، وصيغ بلغة واضحة خالية من التعقيد لتجنب التحيز. يعتمد هذا الاستبيان في قياس استجابات

أفراد العينة على مقياس ليكرت الخماسي (Likert Scale) الذي يعتبر من أكثر المقاييس استخداما وملاءمة للبيانات الترتيبية، حيث يمنح المبحوث مساحة للتعبير عن درجة موافقته وفق التدرج التالي: أوافق بشدة (5)، أوافق (4)، محايد (3)، لا أوافق (2)، لا أوافق بشدة (1).

5. **صدق وثبات الأداة:** يقتضي البحث العلمي الصارم إخضاع أداة القياس لاختبارات قبلية للتأكد من قدرتها على قياس ما أعدت لقياسه فعليا. لتحقيق الصدق الظاهري (صدق المحكمين)، تم عرض الاستبيان في نسخته الأولية على لجنة من الأساتذة المختصين في التسويق وإدارة الأعمال لتقييم مدى وضوح العبارات وارتباطها بالفرضيات، وتم إجراء التعديلات بناء على توجيهاتهم. (محمد بوزيان تيغزة، توجهات حديثة في تقدير صدق وثبات درجات أدوات القياس، (مجلة العلوم النفسية والتربوية)، العدد 01، المجلد 04، جامعة الشهيد حمة لخضر، الوادي الجزائر، 2017، ص 10 .(أما لضمان الثبات والاتساق الداخلي للاستبيان، والمتمثل في إعطاء نفس النتائج لو أعيد تطبيقه في ظروف مماثلة، تم استخدام معامل ألفا كرونباخ .(Cronbach's Alpha) وتعتبر الأداة صالحة ومستقرة للتحليل إذا تجاوزت قيمة المعامل النسبة الإحصائية المقبولة وهي 0.70 للمحاور مجتمعة.

6. **الأساليب الإحصائية المستعملة:** لمعالجة البيانات الخام المسترجعة، تم تفريغ الاستبيانات وتحليلها حاسوبيا باالعتماد على برنامج الحزم الإحصائية للعلوم الاجتماعية .(SPSS V.23) شملت المعالجة استخدام الإحصاء الوصفي كحساب التكرارات والنسب المئوية لوصف الخصائص الديموغرافية، واستعمال المتوسط الحسابي والانحراف المعياري لقياس تشتت الإجابات حول مركز تمثيل البيانات، وتحديد اتجاه الرأي العام للعينة. كما تم توظيف الإحصاء الاستدلالي متمثال في معامل الارتباط بيرسون (Pearson) لاختبار صحة الفرضيات وقياس قوة واتجاه العالقة بين متغيري الدراسة.

سابعا : الدراسات السابقة المحلية

1. دراسة: أهمية حوكمة الأمن السيبراني لضمان تحول رقمي آمن للخدمة العمومية في الجزائر (2022).

- **هدف الدراسة** :تهدف هذه الدراسة إلى تسليط الضوء على دور حوكمة الأمن السيبراني في حماية التحول الرقمي للخدمات العمومية في الجزائر، وتحليل التحديات التي تواجه المؤسسات الجزائرية في هذا المجال.

- **المنهج والأدوات** :اعتمدت الدراسة على المنهج الوصفي التحليلي لمناقشة أطر الأمن السيبراني الوطنية.
- **أهم النتائج** :توصلت الدراسة إلى أن الأمن السيبراني يعد تحدياً كبيراً للمؤسسات الجزائرية، وأن هناك هشاشة في مستوى الأمن السيبراني المبذول مقارنة بتنامي التهديدات الرقمية، مشددةً على ضرورة وجود استراتيجيات حوكمة متكاملة.

2. دراسة: مستوى الوعي السيبيراني في الوسط الجامعي الجزائري وعلاقته بالجريمة الإلكترونية

- **هدف الدراسة** : استقصاء مستوى الوعي لدى الفئات الجامعية بالأمن السيبراني وكيفية تأثير هذا الوعي في الحد من الجريمة الإلكترونية.
- **المنهج والأدوات** : اعتمدت الدراسة على المنهج الوصفي مع استخدام الاستبيان كأداة لجمع البيانات الميدانية.
- **أهم النتائج** : أظهرت الدراسة وجود علاقة ارتباطية بين ضعف الوعي السيبراني وزيادة التعرض للمخاطر الإلكترونية، مؤكدة على أهمية التثقيف الرقمي كخط دفاع أول في بيئة المؤسسات.

1. دراسة : Cybersecurity and Sovereignty: The Balance between National Interests and International Cooperation (2020) – Zargham & Sulaiman.

- **هدف الدراسة** : دراسة التوازن الدقيق بين حماية الأمن السيبراني الوطني (السيادة الرقمية) ومتطلبات التعاون الدولي لمواجهة التهديدات السيبرانية العابرة للحدود.
- **المنهج والأدوات** : اعتمدت الدراسة على المنهج التحليلي المقارن لاستعراض السياسات الدولية.
- **أهم النتائج** : أكدت الدراسة أن حماية البيانات الوطنية تتطلب استراتيجيات مرنة تجمع بين التشريعات المحلية والامتثال للمعايير الدولية، وأن الانغلاق الرقمي ليس حلاً فعالاً لمواجهة التهديدات السيبرانية.

2. دراسة : Cybersecurity Awareness, Knowledge, and Behavior: A Comparative Study (2022) – Basim, H. N.

- **هدف الدراسة** : تحليل الأثر المباشر لوعي ومعرفة الموظفين/المستخدمين بالأمن السيبراني على سلوكهم تجاه حماية البيانات الرقمية.
- **المنهج والأدوات** : المنهج التحليلي الكمي باستخدام دراسة مقارنة.
- **أهم النتائج** : أثبتت الدراسة أن الوعي التقني وحده لا يكفي، بل يجب أن يترجم إلى "سلوك آمن " (Secure Behavior) من خلال التزام الموظفين بسياسات حماية البيانات، وهو ما يقلل بشكل ملحوظ من فرص نجاح الهجمات السيبرانية.
- **علاقة الدراسة الحالية بالدراسات السابقة**

تتميز دراستك الحالية بكونها قيمة مضافة من خلال التكامل التالي:

1. **الشمولية** : بينما ركزت الدراسات المحلية السابقة على قطاعات محددة (الخدمة العمومية أو الوسط الجامعي)، تتوسع دراستك في مفهوم "بيانات العملاء" بصفة عامة، مما يوفر رؤية أوسع وأكثر حداثة.
2. **الربط الاستراتيجي** : تتجاوز دراستك الجانب التقني (الذي تناولته الدراسات السابقة) لتدمج بين الامتثال القانوني، وحوكمة الخصوصية، والمرونة الرقمية، مما يواكب التطورات التشريعية والتقنية الحالية في الجزائر.
3. **التكامل المفاهيمي** : تعتمد دراستك على ما بدأته الدراسات الأجنبية في مجال "السلوك الأمني" والتعاون الدولي، وتسقط هذه المفاهيم على الواقع الميداني الجزائري، مما يجعل البحث جسراً بين النظرية الأكاديمية والممارسة المهنية في بيئة الأعمال الجزائرية.

ثامنا: مخطط الدراسة

للإجابة على الاشكالية قمنا بتقسيم بحثنا إلى 3 فصول كالتالي:

الفصل الأول:

بيانات العملاء

في التسويق الخدماتي

يعيش الفكر الإداري والتسويقي المعاصر تحولات بنيوية عميقة ومتسارعة، مدفوعة بطفرة غير مسبوقة في تكنولوجيا المعلومات والاتصالات. يسمى هذا العصر بعصر تكنولوجيا الاتصال، وعصر الرقمنة، والمعلوماتية، وعصر الوسائط المتعددة، والذكاء الاصطناعي، وكلها مسميات تشير في جوهرها إلى زاوية محددة من انفجار معرفي وتكنولوجي أدى بالضرورة إلى إعادة هندسة طبيعة العلاقة التبادلية بين المنظمات وعملائها[1]. لم يعد السوق مجرد فضاء مادي تلتقي فيه قوى العرض والطلب، بل استحال إلى بيئة افتراضية متشابكة تتدفق عبرها ملايين المعطيات في أجزاء من الثانية. وفي قلب هذا المشهد المعقد، برزت "بيانات العملاء" كأثمن أصل استراتيجي غير ملموس تمتلكه المنظمات الخدمية، محتلة بذلك مكانة الصدارة في توجيه دفة الميزة التنافسية.

تكتسي هذه البيانات طابعاً حيوياً ومفصلياً في قطاع الخدمات على وجه التحديد؛ فالخدمة بطبيعتها اللاملموسة وغير المتجانسة تتطلب من المسوق امتلاك قدرات استباقية خارقة لفهم النوايا الشرائية وتخصيص العروض لتلائم التوقعات الدقيقة لكل زبون على حدة. وتلعب قواعد البيانات دور الذاكرة المؤسسية التي توثق السلوكيات، وترصد التفضيلات، وتقيس مستويات الرضا، مما يسمح للمنظمة بالانتقال من التسويق العشوائي الشامل إلى التسويق التفاعلي والفردي[2]. رغم هذه الأهمية القصوى، فإن تجميع هذه الكتل الهائلة من البصمات الرقمية وتخزينها يضع المنظمة أمام مفارقة استراتيجية حرجة. فبقدر ما تمثل هذه المعلومات مورداً اقتصادياً يدر الأرباح ويبني علاقات ولاء طويلة الأمد، بقدر ما تشكل نقطة ضعف جوهرية ومصدراً لتهديدات وجودية إن لم تُحط بسياج أمني منيع. إن الاستغلال المكثف لهذه المعطيات يفتح الباب واسعاً أمام مخاطر الاختراق، والقرصنة، وسوء الاستخدام الأخلاقي الذي قد يعصف بثقة المستهلك ويدمر السمعة المؤسسية في لحظات معدودة.

تأسيساً على هذا التشابك المعرفي والتطبيقي، يهدف هذا الفصل إلى تفكيك ماهية بيانات العملاء في بيئة التسويق الخدماتي، واستكشاف أبعادها المختلفة. وللإحاطة المنهجية الدقيقة بهذا الموضوع، ارتأينا تقسيم هذا الفصل إلى مبحثين متكاملين؛ يركز المبحث الأول على التأصيل المفاهيمي لبيانات العملاء من حيث التعريف، الأنواع، والخصائص، في حين ينصرف المبحث الثاني إلى تحليل الدور التشغيلي والاستراتيجي لهذه البيانات في اتخاذ القرار التسويقي وبناء العلاقة مع الزبون، وصولاً إلى تشخيص المخاطر المترتبة عن انكشافها وسوء استغلالها.

[1]– ليلى بن برغوث، "الأمن السيبراني وحماية خصوصية البيانات الرقمية في الجزائر في عصر التحول الرقمي والذكاء الاصطناعي"، المجلة الدولية للاتصال الاجتماعي، المجلد 10، العدد 1، 2023، ص 444.

[2]– فلاح عبد الرزاق، وعيسات محمد، "الأمن المعلوماتي كدعامة لتعزيز تطبيقات التسويق الالكتروني دراسة حالة مؤسسة اتصالات الجزائر"، مذكرة مقدمة لاستكمال متطلبات شهادة الماستر، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة ابن خلدون – تيارت، الجزائر، السنة الجامعية 2021–2022.، ص 17

المبحث الأول: الإطار المفاهيمي لبيانات العملاء

يُشكل التحديد الدقيق للمفاهيم والمصطلحات نقطة الانطلاق الأساسية والركيزة العلمية الأولى في أي دراسة أكاديمية، إذ لا يمكن استيعاب الآليات المعقدة لاستغلال وحماية الأصول الرقمية دون تجريدها أولاً من اللبس والغموض المفاهيمي. وفي هذا السياق، لم تعد البيانات مجرد مدخلات حاسوبية أو رموز تقنية صماء، بل تحولت في الفكر التسويقي والتشريعي الحديث إلى امتداد طبيعي لشخصية العميل، تعكس هويته، وتفصح عن سلوكه، وتكشف عن أدق تفاصيل انتمائه المجتمعي والاقتصادي.

إن هذا التحول في النظر إلى المعلومة يفرض علينا مقاربة إبستمولوجية تتجاوز التعريفات الكلاسيكية الجافة، لتبحث في التقاطعات المعقدة بين القانون، والاقتصاد، وتكنولوجيا المعلومات.[1]

تتفرع هذه المعطيات إلى حزمة واسعة من التصنيفات التي تتباين في درجة حساسيتها وطرق تجميعها. فمنها ما يعكس البنية الديموغرافية والجسدية الثابتة للفرد كالمعرفات المباشرة والبيانات البيومترية، ومنها ما يجسد نبضه الحركي المستمر في الفضاءات الافتراضية كبيانات التتبع وتدفق النقر. ويخضع هذا المزيج المعلوماتي الهجين لخصائص اقتصادية وتشغيلية متفردة، كاللاملموسية المطلقة، والقابلية اللانهائية للمقاطعة والدمج، والسرعة الفائقة في التلف إن لم يجرِ تحديثها[2]. وبناءً على ما تقدم، سيكرس هذا المبحث مجهوده التحليلي لضبط المفهوم اللغوي والاصطلاحي لبيانات العملاء، وتتبع دلالاتها في التسويق الحديث، ثم الغوص في تصنيف أنواعها المتعددة، لنختتم ببلورة الخصائص المميزة التي تمنحها تلك القيمة الاستراتيجية وتجعلها في الوقت عينه شديدة الهشاشة.

المطلب الأول: مفهوم بيانات العملاء في التسويق

أولاً: التعريف اللغوي والاصطلاحي

تستند المعرفة الإنسانية في شقها الرقمي المعاصر إلى وحدات بناء أساسية تتدرج في تعقيدها من الشكل الخام إلى الشكل المعالج القابل للاستخدام الاستراتيجي. وتعتبر البيانات في أصلها اللغوي والتقني بمثابة المادة الخام الأولى التي تبنى عليها صروح المعرفة في شتى المجالات. وقد اهتم الباحثون بتفكيك هذا المصطلح وتجريده من اللبس المفاهيمي القائم بينه وبين مصطلحات رديفة كالمعلومات، حيث تمثل

[1]– عمرو طه بدوي محمد، التنظيم القانوني لمعالجة البيانات الشخصية: دراسة تطبيقية على معالجة تسجيلات المراقبة البصرية، دار النهضة العربية للنشر والتوزيع، القاهرة، مصر أو دار النهضة العلمية للنشر والتوزيع، دبي، 2020، ص 205.

[2]– قيبوعة عبد الله، الآليات القانونية لحماية قواعد البيانات في ظل البيئة الرقمية: دراسة مقارنة، أطروحة دكتوراه في الحقوق، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية – أدرار، الجزائر، 2022، ص 16.

البيانات أرقاماً وحقائق غير معالجة وليس لها دلالات أو معنى محدد، والتي تدخل إلى النظام المعلوماتي لتحويلها بشكل معين لتستنبط معانيها واستجلاء سياقها العام أو مضمونها لتصبح معلومات ذات قيمة.[1]

تأخذ هذه المادة الخام أبعاداً قانونية واقتصادية بالغة التعقيد حين يتم ربطها بكيان الفرد، لتتحول من مجرد إشارات حاسوبية مجردة إلى ما يُعرف بـ "البيانات الشخصية". وتتجسد هذه البيانات في كل معلومة عائدة إلى شخص معين يمكن أن تساعد على تحديد هويته والتعرف عليه بشكل قطعي، كالاسم الشخصي، مكان السكن، عنوان الهاتف، رقم البريد الإلكتروني، وغيرها من المعرفات المادية والرقمية التي تتقاطع لتشكل البصمة الفردية للمستهلك في الفضاءات المفتوحة[2]. تتسع دائرة هذا المفهوم في الأدبيات التشريعية الحديثة لتشمل أدق التفاصيل التي قد تفصح عن هوية العميل بصورة غير مباشرة، وهو ما يعكس تطوراً ملموساً في النظرة إلى البيانات كعنصر لصيق بكرامة الفرد وخصوصيته. فالمشرع لم يعد يكتفي بالمعرفات الكلاسيكية، بل امتد تعريفه ليشمل كل ما يشير إلى شخص ما سواء بصفة مباشرة أو غير مباشرة، متضمناً عناصر هويته البدنية، الفسيولوجية، الجينية، الثقافية، والاقتصادية، بالإضافة إلى البيانات الأمنية والائتمانية والموقع الجغرافي.[3]

إن هذا التنوع الهائل في طبيعة المعطيات التي يمكن جمعها عن الأفراد يبرز حجم المخزون المعرفي الذي يمكن استخلاصه، ويؤكد أن اصطلاح "بيانات العملاء" يتجاوز السجلات المحاسبية البسيطة ليغوص في أعماق التكوين المجتمعي للفرد. وتتعاظم حساسية هذه المعطيات في ظل اتساع نطاق استخدام الشبكات المفتوحة، حيث أصبحت حماية هذه البيانات بمثابة التحدي الأكبر الذي يؤرق المنظمات والمستخدمين على حد سواء في عصر الثورة الرقمية.[4]

تحتاج هذه المنظومات البيانية إلى قواعد متطورة لإدارتها، إذ لا قيمة لبيانات العملاء إن ظلت مشتتة أو غير مهيكلة.

[1] – قيبوعة، عبد هلال، الآليات القانونية لحماية قواعد البيانات في ظل البيئة الرقمية – دراسة مقارنة، أطروحة دكتوراه، تخصص القانون الخاص المعمق، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية – أدرار، 2020، ص 09.

[2]– لعياشي حمزة، جعفر محمد الأمين، الأمن السيبراني وحماية البيانات الرقمية في الجزائر، مذكرة ماستر أكاديمي، تخصص قانون الإعلام الآلي والأنترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي – برج بوعريريج، 2021، ص 12.

[3]– أحمد محمد، الملكية الفكرية لقواعد البيانات في القانون السوري والمقارن، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، العدد الثاني، المجلد 29، جامعة دمشق، 2013، ص 15 .

[4]– منى الأشقر جبور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، 2016، ص 25.

وتبرز هنا أهمية تكنولوجيا قواعد البيانات التي تلعب دور الذاكرة الحية للمؤسسة، وهي ذاكرة ديناميكية تسمح بتنظيم كميات هائلة من البيانات وتسهل استرجاعها وتحديثها المستمر لدعم آليات اتخاذ القرار وتوجيه العروض بما يتوافق مع الرغبات الدقيقة للمستهلكين.[1]

بناءً على ما تقدم، يمكن استخلاص أن بيانات العملاء اصطلاحاً هي ذلك المزيج المركب من المعرفات الديموغرافية، السلوكية، والاقتصادية، والتي تُجمع وتُعالج وتُخزن ضمن بيئات رقمية مخصصة، بهدف تكوين صورة شاملة ودقيقة عن العميل تمكّن المنظمة من فهم احتياجاته وتوقع رغباته والتفاعل معه على أسس علمية وموضوعية بعيداً عن العشوائية.[2]

ثانياً: المفهوم التسويقي الحديث لبيانات العملاء

شهد الفكر التسويقي تحولات عميقة وجذرية بالتزامن مع الانفجار المعرفي وتطور تكنولوجيا الاتصال، وهو ما أعاد هندسة المبادئ الأساسية للعلاقة بين المنظمة والزبون. في قلب هذه التحولات، برز مفهوم "المستهلك الرقمي" ككيان تفاعلي شديد الديناميكية، متجاوزاً دوره التقليدي كمتلقٍ سلبي للمنتجات والخدمات. ويُعرف هذا المستهلك الحديث بأنه الشخص الذي ينتقي ويشتري السلع والخدمات ويستهلكها لإشباع حاجاته عن طريق التعاقد بالوسائل الإلكترونية الحديثة، مخلفاً وراءه أثراً رقمياً مستمراً مع كل تفاعل يقوم به.[3]

لم تعد هذه الآثار الرقمية والبيانات المجمعة تُعامل كأرشيف خامل يُحفظ لغايات إدارية فقط، بل أضحت تُعتبر من أثمن الأصول التجارية والاستراتيجية للمنظمات المعاصرة. وتكتسي هذه المعلومات قيمة اقتصادية استثنائية، إذ تعتبر سمات الأفراد مثل العمر، الدخل، التفضيلات، ومسارات التصفح والنقرات، أصولاً تجارية متزايدة الأهمية يتم استغلالها لبلورة استراتيجيات تسويقية موجهة بدقة متناهية.[4]

في قطاع التسويق الخدماتي تحديداً، تكتسي بيانات العملاء طابعاً أكثر خطورة وأهمية مقارنة بتسويق السلع المادية. فالخدمة بطبيعتها تتميز باللاملموسية وعدم التجانس والتلازم بين التقديم والاستهلاك، مما يجعل تقييم العميل لها مبنياً بالدرجة الأولى على جودة التفاعل والثقة المتبادلة. وتلعب البيانات دور الوسيط الذي "يُلمّس" الخدمة ويوجهها لتلائم التوقعات الفردية لكل عميل على حدة، وهو ما

[1]– محاسنة، محمد سلطان ماجد علي، أثر تكنولوجيا قواعد البيانات في اختيار الاستراتيجية التنافسية لشركات الدواء الأردنية، أطروحة دكتوراه، تخصص إدارة الأعمال، كلية الدراسات الإدارية والمالية، جامعة عمان العربية، الأردن، 2007، ص 22.

[2]– قيبوعة، عبد الله، مرجع سبق ذكره، ص 11.

[3]– فلاح عبد الرزاق، عيسات محمد، تسويق الخدمات، مذكرة ماستر أكاديمي، تخصص تسويق الخدمات، قسم العلوم التجارية، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة ابن خلدون – تيارت، 2023، ص 10.

[4]– أحمد ياسين نجلاء، الرقمنة وتقنياتها في المكتبات العربية، دار العربي للنشر والتوزيع، القاهرة، 2014، ص 45.

يعزز قدرة المنظمة الخدمية على بناء علاقات طويلة الأمد وتجنب تقديم وعود لا تتطابق مع حاجات الزبون الحقيقية.[1]

يتجسد هذا التوجه الاستباقي بوضوح بالغ من خلال الاعتماد على تقنيات تتبع سلوكيات المستخدمين، مثل تحليل بيانات تدفق النقر والاعتماد على ملفات تعريف الارتباط. فهذه التقنيات تتيح للمنظمة الخدمية جمع تفاصيل دقيقة عن سلوك التصفح الأساسي للعميل، بما في ذلك الصفحات التي أثارت اهتمامه، والوقت الذي استغرقه في قراءة وصف خدمة معينة، مما يوفر لوحة تحكم استراتيجية تقرأ نوايا العملاء حتى قبل أن يصرحوا بها، وتسمح بتقديم عروض شخصية لحظية تلبي تلك النوايا بكفاءة.[2]

يتيح هذا الفهم المعمق لبيانات العملاء الانتقال السلس نحو تبني منهجيات "التسويق التفاعلي"، والذي يُعد نموذجاً متطوراً يعتمد بشكل مكثف على جودة تدفق المعلومات بين الطرفين. يهدف هذا النموذج إلى خلق حوار ثنائي الاتجاه يبني علاقة قوية بين مقدم الخدمة والزبون، مستفيداً من انخفاض تكلفة الاتصال عبر الشبكات الرقمية وسرعتها.

وكلما زادت دقة البيانات المجمعة وتحليلها، أصبح هذا التفاعل سياقياً وذا قيمة مضافة للعميل، بدلاً من أن يكون تدخلاً مزعجاً في مساحته الشخصية.[3]

مع هذا الاعتماد الجذري على قواعد البيانات في تصميم السياسات التسويقية وإدارة علاقات العملاء، تتولد مفارقة حرجة تتمثل في حجم المخاطر المرتبطة بهذه الأصول. إن تجميع هذه الكتل الضخمة من البيانات الشخصية والحساسة يجعل من المنظمات الخدمية أهدافاً مغرية للتهديدات والاختراقات في الفضاء الرقمي. ففقدان هذه البيانات أو تسريبها لا يمثل مجرد خسارة تقنية، بل هو انهيار مباشر لمقومات الاستراتيجية التسويقية وضرب لسمعة المؤسسة التي تُبنى على

عامل الثقة.[4]

يدفعنا هذا الواقع التشغيلي المعقد إلى الإقرار بأن المفهوم التسويقي الحديث لبيانات العملاء لم يعد قابلاً للفصل بأي شكل من الأشكال عن مفاهيم الحماية والأمن. فالمنظمة التي تستثمر الملايين في بناء أنظمة ذكية لجمع البيانات وتحليل سلوكيات العملاء، تقف عاجزة عن الاستفادة من هذه الأصول إن لم

[1]– فلاح عبد الرزاق، عيسات محمد، المرجع السابق، ص 15

[2]– بكيس عبد الحفيظ، عبدو رشيدة، خضر رحاب، حفظ أمن المعلومات في ظل الذكاء الإصطناعي، مذكرة ماستر أكاديمي، تخصص قانون إعالم آلي وأنترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي – برج بوعريريج، 2023، ص 24.

[3]– برادة عبد الرزاق، مستوى الوعي السيبيراني في الوسط الجامعي الجزائري وعلاقته بالجريمة الإلكترونية، أطروحة دكتوراه، تخصص علم الاجتماع الجريمة والانحراف، كلية العلوم الإنسانية والاجتماعية، جامعة خميس مليانة، دون سنة نشر، ص 193 .

[4]– نوفيل حديد، كربيط حنان، أمن المعلومات ودوره في مواجهة الاعتداءات الالكترونية على نظام معلومات المؤسسة، مجلة العلوم الاقتصادية والتجارية وعلوم التسيير، العدد 3، المجلد 3، جامعة الجزائر 3، 2014، ص 50 .

توفر لها درعاً واقياً يصد الهجمات المتطورة. ومن هنا يتجلى التداخل العضوي بين إدارة التسويق الخدماتي وإدارة الأمن السيبراني كحتمية استراتيجية لبقاء المؤسسة ونموها المستدام.[1]

تُظهر الممارسات التسويقية المعاصرة أن وعي العملاء بمدى قدرة المؤسسة على حماية بياناتهم أصبح يشكل معياراً حاسماً في قراراتهم الشرائية. لم يعد التنافس مقتصراً على جودة الخدمة المقدمة أو سعرها، بل امتد ليشمل "الموثوقية الرقمية". فالعميل الذي يدرك أن المنظمة تمتلك بنية سيبرانية قادرة على التصدي لمخاطر الاستخدام غير المشروع لمعلوماته، يميل إلى تطوير ولاء مؤسسي أعمق والتزام أقوى بخدمات تلك المنظمة، مما ينعكس إيجاباً على المردودية الاقتصادية والحصة السوقية بشكل عام.[2]

إن استدامة العمليات التسويقية في بيئة تتسم بالتغير التقني المتسارع تتطلب من متخذي القرار في المنظمات الخدمية النظر إلى بيانات العملاء من منظور مزدوج: الأول يراها كأداة لخلق القيمة وتصميم الخدمات، والثاني يعتبرها أمانة قانونية وأخلاقية تتطلب تفعيل أقصى درجات الحيطة الأمنية. هذا التوازن الدقيق هو ما يحول التهديدات المحتملة في البيئة الرقمية إلى فرص لتعزيز الثقة المجتمعية وإثبات الكفاءة المؤسسية.[3]

المطلب الثاني: أنواع بيانات العملاء

تتجاوز المنظمات الخدمية المعاصرة النظرة الأحادية للعميل بوصفه مجرد مستهلك نهائي، لتتعامل معه ككيان معلوماتي معقد يُنتج باستمرار تدفقات هائلة من المعطيات المتنوعة. إن الفهم الدقيق لطبيعة هذه البيانات يمثل حجر الزاوية في بناء أي استراتيجية تسويقية فعالة، فضلاً عن كونه الخطوة التأسيسية الأولى لتصميم سياسات أمنية سيبرانية قادرة على حماية هذه الأصول الرقمية. تتفرع بيانات العملاء إلى فئات متداخلة ومتباينة من حيث درجة الحساسية، وطريقة الجمع، والقيمة الاستراتيجية التي تقدمها لمقدم الخدمة، ويمكن تصنيفها منهجياً وعملياً إلى مسارين رئيسيين يعكسان الجانب التكويني والجانب الحركي للزبون.

أولاً: البيانات الديموغرافية والشخصية.

يُشير هذا الصنف إلى مجموعة الخصائص الثابتة نسبياً والسمات التكوينية التي تُعرّف الفرد وتحدد هويته وموقعه داخل النسيج المجتمعي والاقتصادي. تمثل هذه المعطيات القاعدة المرجعية التي تبني

[1]– بارة سميرة، الأمن السيبراني في الجزائر، السياسات والمؤسسات، المجلة الجزائرية للأمن الإنساني، العدد 4، جامعة قاصدي مرباح – ورقلة، 2017، ص 12 .

[2]– علاء الدين فرحات، الفضاء السيبراني تشكيل ساحة المعركة في القرن الحادي والعشرين، مجلة العلوم القانونية والسياسية، العدد 03، المجلد 10، المدرسة الوطنية العليا للعلوم السياسية، الجزائر، 2019، ص 20 .

[3]– غياث بوفلجة، التربية والتعليم في الجزائر، ط1، دار الغرب للنشر والتوزيع، الجزائر، 2008، ص 40.

عليها المؤسسات الخدمية ملفات عملائها .(Customer Profiles) وتُعرّف البيانات الشخصية في أبسط صورها بأنها كافة المعلومات التي تشير إلى شخص ما بطريقة واضحة ومباشرة، متضمنة الاسم الكامل، وأرقام الهوية الوطنية، وعناوين السكن، وأرقام الهواتف، وعناوين البريد الإلكتروني.[1]

من منظور أمني وتحليلي، يقسم الباحثون هذه المعطيات الديموغرافية والشخصية إلى مستويات متدرجة بناءً على قدرتها على كشف هوية الزبون. تبرز في المستوى الأول "المعرفات المباشرة القوية " (Strong Identifiers) وهي تلك المعطيات التي تستقل بذاتها في تحديد كينونة فرد واحد دون سواه في أي قاعدة بيانات، مثل أرقام جوازات السفر، والأرقام التأمينية والضريبية، والبطاقات الائتمانية. وفي المستوى الثاني نجد "المعرفات شبه المباشرة" أو "المعرفات الضعيفة (Quasi-identifiers) "، والتي تشمل متغيرات ديموغرافية عامة كالعمر، والجنس، والرمز البريدي، ومستوى الدخل، والمنطقة الجغرافية، ورغم أن هذه المعطيات لا تكشف هوية الفرد بمفردها، إلا أن دمجها ومقاطعتها حاسوبياً يقود حتماً إلى التعرف الدقيق على العميل وإعادة بناء هويته الرقمية بالكامل.[2]

تكتسي هذه الهيكلة المزدوجة للمعرفات أهمية بالغة في التسويق الخدماتي، حيث تعتمد المنظمات على المعرفات شبه المباشرة لتقسيم السوق إلى شرائح متجانسة (Market Segmentation) ، وتستخدم المعرفات القوية لإتمام عمليات التعاقد والفوترة.

بموازاة ذلك، يتسع نطاق البيانات الديموغرافية والشخصية ليحتضن فئة بالغة الخطورة تُعرف بالبيانات الحساسة .(Sensitive Data) ويشمل هذا التصنيف العميق خصائص تمس الجوهر الإنساني والعقائدي والعرقي للعميل، إذ تتضمن معلومات حول الأصل العرقي أو القبلي، والمعتقدات الدينية أو الفكرية، والعضويات في مؤسسات المجتمع المدني، والبيانات الجنائية والأمنية، فضلاً عن السجلات الائتمانية وبيانات الحالة الصحية والطبية.[3]

تفرض هذه الفئة تحديات أخلاقية وقانونية جسيمة على المسوقين، فبينما تسعى المؤسسات الخدمية (كالمستشفيات، وشركات التأمين، والمؤسسات المالية) لجمع هذه البيانات لتقديم خدمات شديدة

[1]– IT Pillars. 2025. Saudi Personal Data Protection Law: Definition and how to comply. IT Pillars ManageEngine & Zoho Partner in Saudi Arabia. Retrieved from https://www.it-pillars.com/ar/blog-ar/نظام-حماية-البيانات-السعودي/

[2]– Utrecht University. 2025. K-anonymity, l-diversity and t-closeness. Data Privacy Handbook. GitHub Pages. Retrieved from https://utrechtuniversity.github.io/dataprivacyhandbook/k-l-t-anonymity.html

[3]– نفس المرجع السابق، ص 1

التخصيص، تجد نفسها أمام ترسانة من القوانين التي تمنع معالجة هذه المعطيات دون موافقة صريحة، نظراً لما قد يترتب على تسريبها من تمييز عنصري أو إضرار بالغ بالسمعة الشخصية للعميل.[1]

لم تتوقف حدود البيانات الشخصية عند المعرفات الورقية أو السجلات الكلاسيكية، بل امتدت بقوة نحو الخصائص الفسيولوجية والبيولوجية للفرد بفضل التقدم التكنولوجي، لتبرز "البيانات البيومترية" كعنصر محوري في هذا التصنيف. تتضمن المعطيات البيومترية تفاصيل فيزيائية لا يمكن تكرارها أو استنساخها بسهولة، مثل البصمات الحيوية، والحمض النووي (DNA) ، ومسح قزحية العين، وبصمات الصوت، والخصائص الهندسية للوجه.[2]

يُعد توظيف البيانات البيومترية في العمليات التسويقية والخدمية، كاستخدام بصمة الوجه لتأكيد الدفع الإلكتروني أو بصمة الصوت لتمرير أوامر بنكية، نقلة نوعية تهدف إلى تقليل الاحتكاك المادي وتسريع وتيرة الخدمة (Frictionless Service) ، إلا أنها في الوقت عينه تحول العميل مادياً إلى "بيانات حية"، مما يجعل اختراق قواعد البيانات البيومترية كارثة حقيقية؛ فكلمة المرور المسروقة يمكن تغييرها، أما البصمة الفسيولوجية المسروقة فتظل مخترقة للأبد، مما يضع أنظمة الأمن السيبراني أمام اختبار وجودي غير مسبوق.

ثانياً: البيانات السلوكية والتفاعلية.

إذا كانت البيانات الديموغرافية تجيب على سؤال "من هو العميل؟"، فإن البيانات السلوكية والتفاعلية تجيب بشمولية وعمق على سؤال "ماذا يفعل العميل؟ وكيف يتصرف؟". يجسد هذا النوع من البيانات البصمة الديناميكية والأثر الرقمي الذي يخلفه المستهلكون وراءهم أثناء تنقلهم وتفاعلهم داخل البيئات الافتراضية والمنصات الخدمية. ولا تمثل هذه المعطيات أرشيفاً لماضٍ منتهٍ، بل هي مؤشرات حيوية ونبض رقمي مستمر تستخلصه الخوارزميات للتنبؤ بالنوايا الشرائية المستقبلية وتوجيه السلوك الاستهلاكي بكفاءة عالية.[3]

تأتي "بيانات تدفق النقر (Clickstream Data) "في طليعة هذه الفئة، وهي المعلومات الانسيابية الدقيقة التي تجمعها المنظمات بناءً على سلوك التصفح الأساسي لعملائها. يتضمن ذلك توثيقاً محكماً لرحلة الزبون داخل الموقع الخدمي، شاملاً الصفحات التي شاهدها، والمدة الزمنية التي قضاها في كل

[1]– Cochran, K. A. 2024. Cybersecurity Essentials: Practical Tools for Today's Digital Defenders 1st ed.. Apress, p. 276.

[2]– Whitman, M. E., & Mattord, H. J. 2017. Principles of Information Security 6th ed.. Cengage Learning, p. 143.

[3]– Acquisti, A., Taylor, C., & Wagman, L. 2016. The Economics of Privacy. Journal of Economic Literature, 542, 442.

صفحة(Dwell Time) ، ومسارات التصفح(Browsing Paths) ، وعنوان بروتوكول الإنترنت (IP Address)، والروابط التي فضل النقر عليها متجاوزاً غيرها.[1]

هذا التحليل المجهري للحركات الرقمية يسمح لإدارة التسويق بتشخيص "نقاط الألم (Pain Points)" لدى الزبون، ومعرفة اللحظة الدقيقة التي تراجع فيها عن طلب الخدمة، مما يتيح التدخل الفوري لتقديم حوافز تسويقية أو تعديل واجهة العرض لتلائم توقعاته اللحظية.

تكتسب هذه البصمة السلوكية عمقاً إضافياً من خلال التفاعلات الاجتماعية والتقييمات الرقمية التي يشاركها العميل طواعية. وتُعرف هذه التفاعلات بالكلمة المنطوقة إلكترونياً(eWOM) ، وتتجسد في التعليقات، المراجعات، النقاشات الحوارية، والتفضيلات التي ينشرها الزبائن على المدونات، والمنتديات، ومواقع التواصل الاجتماعي، وصفحات العلامات التجارية.[2]

تكشف هذه النصوص التفاعلية عن المشاعر، والمواقف النفسية، والانتماءات الثقافية للعميل تجاه الخدمة المقدمة، وتعتبر من أقوى أنواع البيانات السلوكية لأنها تعكس رأياً صريحاً وقناعة ذاتية تؤثر بشكل مباشر ومعدٍ على قرارات شريحة واسعة من العملاء المرتقبين الذين يراقبون هذه الحوارات ويتبنون مضامينها لتخفيض حالة عدم التأكد المرتبطة باستهلاك الخدمات غير الملموسة.

تتغذى المنظومة التسويقية المعاصرة على أدوات برمجية متطورة لجمع هذه البيانات التفاعلية بصفة خفية ومستمرة عبر المواقع المتعددة. تعتمد المنظمات بشكل مكثف على برمجيات التتبع (Tracking Technologies)كملفات تعريف الارتباط (Cookies) وإشارات الويب أو حشرات الويب (Web Bugs/Beacons)تعمل هذه البرمجيات كجواسيس رقمية تُزرع في متصفح العميل أو داخل رسائل البريد الإلكتروني، لتقوم بمراقبة نشاطاته عبر مختلف الشبكات، وقياس فعالية الإعلانات، وتحليل استجاباته للعروض الترويجية، حتى دون أن يدرك ذلك.[3]

يُتيح هذا التتبع العميق للمسوقين تصميم شبكات إعلانية فائقة الدقة تستهدف الزبون بخدمات محددة تتطابق مع عمليات بحثه الأخيرة، وهو ما يعزز العوائد المالية للمؤسسة من جهة، ولكنه يضعها من جهة أخرى في مواجهة انتقادات حادة تتعلق بانتهاك الخصوصية، ما لم توفر آليات شفافة تمنح العميل حق قبول أو رفض هذا الاستنزاف المستمر لمعطياته السلوكية.

[1]–أليساندرو أكويستي وآخرون، اقتصاديات الخصوصية، مرجع سبق ذكره، ص 205.

[2]–كريستيان تشيونغ وآخرون، تأثير الكلمة المنطوقة إلكترونيا – تبني الآراء عبر الإنترنت في مجتمعات العملاء، مجلة أبحاث الإنترنت، العدد 18، Emerald Group Publishing، 2008، ص 232.

[3]– أليساندرو أكويستي وآخرون، اقتصاديات الخصوصية، مرجع سبق ذكره، ص 202.

في سياق التحولات التكنولوجية المتسارعة، برز نوع جديد وحساس جداً من البيانات التفاعلية، والمتمثل في تفاعل المستهلكين مع أنظمة الذكاء الاصطناعي والنماذج اللغوية الكبيرة .(LLMs) يقوم المستهلكون المعاصرون بإجراء حوارات تفصيلية وطرح استفسارات شخصية دقيقة على روبوتات الدردشة الذكية لطلب المشورة أو تخصيص الخدمة. وقد أثبتت الدراسات أن جودة هذا التفاعل الذكي (من حيث الاستجابة والتخصيص) تساهم في رفع مستوى الثقة والألفة لدى المستهلك، ولكنها في المقابل ترفع من سقف مخاوفه المتعلقة بالخصوصية، نظراً لإدراكه بأن هذه الخوارزميات تقوم بتسجيل، وتحليل، وحفظ أدق تفاصيل حواراته واهتماماته لاستخدامها في تحسين نماذج التوصية وتشكيل نواياه الشرائية المستقبلية. (أحمد يحيى شاهين وآخرون، التجارة الإلكترونية المستدامة في الشرق الأوسط وشمال أفريقيا: تحليل لنية الشراء لدى الجيل Z من خلال تفاعلات النماذج اللغوية الكبيرة مفتوحة المصدر، الثقة، والألفة ومخاوف الخصوصية،[1]

يؤدي الاستثمار المؤسسي في تجميع هذه الفئات المتنوعة من البيانات السلوكية والتفاعلية إلى الدفع بعجلة "التحول الرقمي لعمليات التسويق والمبيعات"، وهو نموذج يعتمد جذرياً على الأدوات الرقمية لتوطيد استراتيجيات التعامل مع السوق. ويتضمن هذا التحول دمج منصات التجارة الإلكترونية، وشبكات التواصل، والتسويق عبر البريد الإلكتروني لفهم الاحتياجات المتغيرة للزبائن، وتحسين التجربة الاستهلاكية لتصبح تجربة فردية متفوقة ومدعومة بقدرات الذكاء الاصطناعي القادرة على قراءة التوقعات بدقة تامة.[2]

نستخلص مما سبق أن البيانات التي تتعامل معها المنظمات الخدمية لم تعد مجرد أرقام إحصائية جافة، بل هي مزيج هجين ومعقد يجمع بين التكوين المادي والنفسي للعميل (بيانات ديموغرافية وشخصية وبيومترية)، وبين نشاطه وحركته الرقمية المستمرة (بيانات سلوكية وتفاعلية وتقييمية). إن هذا الاندماج البياني يشكل ثروة استراتيجية تضمن للمنظمة التفوق التنافسي والقدرة على ابتكار خدمات غير مسبوقة، ولكنه يضعها في الوقت ذاته فوق صفيح أمني ساخن. فكلما تضخمت تفاصيل هذه البيانات وازدادت دقتها، تعاظمت جاذبيتها للقراصنة ومجرمي الفضاء السيبراني، مما يجعل بناء جدران حماية فولاذية وبروتوكولات أمنية استباقية شرطاً أساسياً لضمان عدم تحول هذه الميزة التسويقية إلى ثغرة مدمرة تعصف بكيان المنظمة ومصداقيتها.

---

[1]– Shaheen, A., Omeish, F., AlGhamdi, D. S., Khataan, A., & Awad, A. 2026. Sustainable E-Commerce in MENA: An SOR Analysis of Gen Z Purchase Intentions through Open-Source LLM DeepSeek Interactions, Trust, Familiarity, and Privacy Concerns. World Journal of Entrepreneurship, Management and Sustainable Development WJEMSD, 221-2, WASD, 133.

[2]– بوحفص، حنان، "الأمن السيبراني بين التحول الرقمي والقصور التشريعي: دراسة تحليلية للإطار القانوني الجزائري"، حوليات جامعة الجزائر 1، المجلد 39، جامعة الجزائر 1 بن يوسف بن خدة، الجزائر، 2025، ص 45.

المطلب الثالث: خصائص بيانات العملاء التسويقية

تكتسي البيانات في بيئة التسويق الخدماتي المعاصر طبيعة استثنائية ومعقدة تميزها بشكل جذري عن باقي الأصول والموارد الكلاسيكية التي تعتمد عليها المنظمات في تسيير أعمالها. إن هذه المعطيات الرقمية لم تعد تعامل كمجرد مخرجات ثانوية للعمليات التبادلية أو سجلات محاسبية تحفظ لغايات التوثيق، بل تحولت في ظل الاقتصاد المبني على المعرفة إلى مدخلات استراتيجية حية، تتسم بتعقيد بنيوي ووظيفي يجعل من الفهم الدقيق لخصائصها خطوة حتمية تسبق أي محاولة لاستغلالها تجارياً أو توفير الحماية السيبرانية لها.

وبناءً على التداخل العميق القائم بين متطلبات التسويق التفاعلي وتكنولوجيا قواعد البيانات، لا يمكن دراسة بيانات العملاء ككتلة صماء، بل يجب تفكيكها إلى نسق من الخصائص الجوهرية المترابطة التي تعكس ديناميكيتها وتفسر قيمتها التنافسية وحساسيتها الأمنية في آن واحد، وتتجلى هذه الخصائص المتسلسلة فيما يلي:

- **اللاملموسية والطبيعة الاقتصادية المتفردة (انعدام التنافسية الاستهلاكية** :(تتميز بيانات العملاء، عند إخضاعها للتحليل كسلع اقتصادية، بخصائص فريدة تبتعد بها تماماً عن السلع المادية المحسوسة. من أبرز هذه السمات ما يُعرف اقتصادياً بـ "انعدام التنافسية (Non-rivalry) "في الاستهلاك. يرتكز هذا المبدأ على حقيقة أن استغلال إدارة التسويق لملف بيانات عميل معين من أجل تصميم حملة ترويجية مخصصة، لا يمنع إطلاقاً إدارة خدمة العملاء أو إدارة المبيعات من استخدام نفس البيانات في اللحظة ذاتها، وبنفس الجودة والفعالية.[1] هذه اللاملموسية العميقة تجعل البيانات قابلة للاستنساخ، والمشاركة، والتوزيع اللانهائي داخل أروقة المنظمة بتكلفة حدية تقارب الصفر. وهذا ما يضاعف من قيمتها الاقتصادية ويجعلها المورد الوحيد الذي لا ينضب بكثرة الاستخدام، بل تتزايد قيمته التراكمية. غير أن هذه الخاصية بالتحديد هي التي تفرز التحدي الأمني الأكبر؛ إذ يمكن تسريب هذه الأصول أو استنساخها خلسة من قبل قراصنة الفضاء السيبراني ونقلها عبر الشبكات المفتوحة دون أن تترك أثراً مادياً يدل على فقدانها، مما يجعل اكتشاف الاختراقات عملية معقدة تتطلب يقظة تكنولوجية فائقة.

[1]– أليساندرو أكويستي وآخرون، مرجع سبق ذكره، ص 194.

- **الدقة والموثوقية العالية كشرط للفعالية** :يرتبط نجاح أي قرار استراتيجي في حقل التسويق الخدماتي بمدى تمتع قواعد البيانات بخاصية الدقة المتناهية. وتعبر الدقة من المنظور التقني والتسويقي عن خلو المعطيات من الأخطاء والتشوهات، وامتلاكها للقيمة الفعلية التي يتوقع المسوق إيجادها والاعتماد عليها.[1]

- في قطاع الخدمات، حيث تبنى الوعود الترويجية على الفهم العميق لحاجات الزبون، تؤدي البيانات غير الدقيقة (سواء كانت أخطاء إملائية في العناوين، أو تصنيفات خاطئة للرغبات) إلى توجيه عروض غير مناسبة، وهو ما يُعرف بـ "العمى التسويقي" الذي يدمر ثقة الزبون ويبدد ميزانية الترويج .تتكامل هذه الدقة مع خاصية "الموثوقية والأصالة"، والتي تعني أن البيانات مستقاة من مصادر حقيقية وغير مختلقة. وتبرز أهمية هذه الخاصية بشدة عند تحليل التقييمات الرقمية وتفاعلات العملاء (الكلمة المنطوقة إلكترونياً)، حيث يمثل إدراك المستخدم لصحة المعلومات، ومدى خلوها من التلاعب المتعمد، حجر الزاوية في بناء العلاقة التفاعلية وتقليل حالة عدم التأكد المرتبطة باستهلاك الخدمات.[2]

- **التوقيت الزمني، الحركية، وسرعة التلف** :لا تعيش بيانات العملاء التسويقية في فراغ زمني ساكن، بل هي سريعة التلف وفاقدة للصلاحية إن لم تخضع لعمليات تحديث مستمرة. تتعلق خاصية "التوقيت" بمدى حداثة الرسائل والمعلومات التي يتم التقاطها، ومدى قدرتها على عكس اللحظة الآنية لتفكير المستهلك. في البيئات الرقمية المتسارعة، إذا لم يتم تزويد قواعد البيانات بمدخلات حية ومستمرة، فإنها ستعجز حتماً عن تقديم الأداء المتوقع، ولن توفر أي قيمة مضافة لمتخذ القرار الذي يبحث عن اقتناص الفرص اللحظية.[3] تعكس هذه الحركية الطبيعة المتقلبة لسلوك المستهلك الرقمي الذي تتغير تفضيلاته وتوجهاته يومياً بل وفي أجزاء من الثانية. هذا ما يفرض على المنظمة الخدمية امتلاك أنظمة تتبع ديناميكية، مثل تحليل بيانات تدفق النقر، لضمان توافر المعلومات الاستباقية في الوقت المناسب تماماً للتأثير على النوايا الشرائية قبل أن تتجه نحو المنافسين.

- **الشمولية التشغيلية والملاءمة السياقية** :تشير خاصية الشمولية إلى درجة اكتمال وتفصيل المعلومات المجمعة حول العميل لتكوين رؤية شاملة (محورها 360 درجة). كلما كانت البيانات غنية

[1]– ميشيل ويتمان، هربرت ماتورد، مرجع سبق ذكره، ص 14.

[2]– كريستيان تشيونغ وآخرون، مرجع سبق ذكره، ص 232.

[3]– نفس المرجع السابق، ص 232.

وعميقة وتغطي كافة نقاط التماس بين الزبون والمنظمة، اتسع نطاق الفئات الاستهلاكية التي يمكن دراستها، وازدادت القدرة على التوجيه الشخصي الدقيق للخدمة.[1]

- غير أن هذه الشمولية المعرفية تظل مجرد تكديس عشوائي إن لم تقترن بشكل وثيق بخاصية "الملاءمة". فالمسوق المحترف لا يبحث عن فوضى المعلومات، بل يحتاج إلى استخلاص البيانات التي ترتبط ارتباطاً مباشراً وعضوياً بالهدف الترويجي المطروح. إن فلترة كتل البيانات الضخمة لاستخراج الأنماط السلوكية الأكثر ملاءمة وسياقية، هي ما يمنح المؤسسة قدرة على الاستجابة السريعة دون إهدار للجهد أو الوقت في تحليل متغيرات ديموغرافية أو تفاعلية لا تخدم القرار الفوري.

- **الاستقلالية والقدرة على إعادة الهيكلة المنطقية** :من زاوية تكنولوجية هيكلية، تتسم النظم التي تدير بيانات العملاء بخاصية الاستقلالية الفائقة، حيث يكرس التصميم الحديث فصلاً قاطعاً بين البيانات في ذاتها، وبين الهياكل المادية والبرمجية المعقدة المخصصة لتخزينها في الخوادم.[2] هذا الانفصال ليس مجرد تفصيل تقني، بل هو ميزة تسويقية جبارة. فهو يسمح لتطبيقات التسويق الإلكتروني وإدارة علاقات العملاء (CRM) باسترجاع البيانات، وإعادة ترتيبها منطقياً، وتوليد تقارير متقاطعة بمرونة مطلقة تتوافق مع حاجات كل قسم داخل المؤسسة، وذلك دون الحاجة إلى إحداث أي تغيير أو تعديل على البنية التحتية الفيزيائية لقاعدة البيانات الأصلية. هذا التنظيم المنطقي القابل للتشكيل المستمر يضمن انسيابية العمليات ويسرّع من وتيرة طرح الخدمات المبتكرة.

- **الحساسية السياقية والقابلية للمقاطعة التراكمية (الدمج** :(تُعد هذه الخاصية من أشد سمات البيانات التسويقية تعقيداً وخطورة. إن القيمة التحليلية، وكذا الحساسية الأمنية لجزء معين من المعلومات، تتغير بشكل جذري ودرامي بناءً على ما يتم دمجه معه من أجزاء أو متغيرات أخرى. فعلى سبيل المثال، قد لا تكشف معلومة جغرافية عابرة أو تفضيل ترفيهي بسيط بشكل منفرد عن هوية العميل أو عن قدرته الائتمانية .ولكن، عندما يتم مقاطعة هذه المعطيات الفرعية (المعرفات شبه المباشرة) وتجميعها عبر خوارزميات الذكاء الاصطناعي، يتولد لدى المسوقين، وكذا لدى المخترقين المحتملين، قدرة مخيفة على إعادة بناء هوية الفرد بالكامل والتنبؤ بأدق تفاصيل حياته[3]. هذه القابلية للمقاطعة والدمج التراكمي هي

[1]– نفس المرجع السابق، ص 232.

[2]– قيبوعة، عبد هلا، مرجع سبق ذكره، ص 42.

[3]– أليساندرو أكويستي وآخرون، مرجع سبق ذكره، ص 194.

المولد الأساسي والمحرك الفعلي لاستراتيجيات الاستهداف الإعلاني الدقيق، وهي ذاتها التي تثير أعمق هواجس انتهاك الخصوصية في العصر الرقمي.

- **المنفعة والتوجه القصدي** :(Utility) في القاموس التسويقي، لا تكتسب السلاسل الرقمية، والرموز، ومدخلات النظام صفة "بيانات تسويقية أصلية" إلا إذا تضمنت خاصية المنفعة المطلقة. تُعرف المنفعة هنا بأنها الحالة التي تكون فيها المعلومات ذات قيمة واضحة، ولها القدرة على خدمة غاية تشغيلية أو استراتيجية محددة. فإذا كانت كميات هائلة من المعلومات متاحة، ولكنها مخزنة بتنسيق غير قابل للقراءة أو غير قابل للتحليل من قبل المسوق النهائي، فإنها تفقد نفعها وتتحول إلى عبء ميت.[1]

- البيانات السلوكية الخام، كأوقات بقاء الزبون في الموقع، قد تبدو للوهلة الأولى مجرد أرقام تقنية مربكة، ولكن عند إخضاعها لمعالجة منهجية تكشف عن "نقاط الألم" والتفضيلات الخفية للعميل، فإنها تتحول إلى معرفة نافعة تمتلك قدرة فائقة على توجيه مسار تصميم الخدمة. هذا التوجه القصدي يؤكد أن حيازة المنظمة للبيانات ليس غاية في حد ذاته، بل هو وسيلة حتمية مبررة بالقدرة على توليد عوائد ملموسة. [2]

- **توليد التباين المعلوماتي** :(Information Asymmetry) تُحدث آليات جمع البيانات التسويقية واستغلالها المكثف تحولاً سيكولوجياً واقتصادياً يتمثل في قلب موازين "التباين المعلوماتي" بين طرفي العلاقة التبادلية. في النماذج الكلاسيكية، يمتلك المستهلك الوعي الأكبر حول رغباته الدفينة وقدرته على الدفع، في حين يعاني البائع من نقص هذه المعلومات. أما في البيئة الرقمية، وبفضل الخصائص المتراكمة للبيانات من شمولية ودقة وقابلية للمقاطعة، يصبح المسوق هو الطرف المهيمن معرفياً .يمتلك مقدم الخدمة عبر تحليلاته العميقة رؤية استباقية تمكنه من فهم نوايا المستهلك، وربما توقع ردود أفعاله المستقبلية وقراراته الشرائية بشكل يفوق الإدراك الواعي للمستهلك نفسه. في المقابل، يبقى الزبون في حالة جهل شبه تام بالكيفية التي ستُعالج بها بياناته، وما هي الخوارزميات التي صاغت له هذا العرض المخصص.[3] يمنح هذا التباين المنظمة الخدمية سلطة تأثير ناعمة وجبارة، مما يضع على عاتقها مسؤولية قانونية وأخلاقية صارمة لمنع التعسف في استخدام هذا التفوق المعرفي.

[1]– ميشيل ويتمان، هربرت ماتورد، مرجع سبق ذكره، ص 14.

[2]– مقدر نبيل، مرجع سبق ذكره، ص 326.

[3]– أليساندرو أكويستي وآخرون، مرجع سبق ذكره، ص 194.

• **الهشاشة المفرطة وحتمية الدرع الأمني** :كنتيجة حتمية لكل الخصائص السالفة الذكر، من قيمة اقتصادية متضخمة، وقابلية للنسخ، وحساسية ناجمة عن الدمج، وقوة في التوجيه السلوكي، تتسم بيانات العملاء بخاصية "الهشاشة المتأصلة .(Inherent Vulnerability) "إنها أصول حية تتدفق عبر شبكات غير مرئية، مما يجعلها عرضة للانتهاك، أو التعديل الخبيث، أو التدمير الشامل في أي لحظة تغيب فيها الجدران الواقية .هذه الهشاشة تحول قواعد بيانات العملاء إلى الغنيمة الاستراتيجية الأبرز التي تسعى الفواعل الإجرامية في الفضاء السيبراني للاستحواذ عليها أو تشفيرها لغايات الابتزاز. وبناءً عليه، يفرض الفكر المؤسسي الحديث ضرورة عدم الاكتفاء بالنظرة التسويقية التوسعية لجمع المعطيات، بل يُلزم متخذي القرار بإرساء بروتوكولات أمنية سيبرانية تضمن ثلاثة ركائز أساسية لاستدامة هذه الخصائص: ضمان "السرية" لحجب البصمة الرقمية عن غير المصرح لهم، وضمان "السلامة" لبقاء النوايا التفاعلية للزبون دقيقة وغير مشوهة، وضمان "التوافر" لتمكين المسوق من الوصول لبياناته وقت اتخاذ القرار.[1]

يُستنتج مما سبق بوضوح، أن خصائص بيانات العملاء التسويقية تتشابك لتشكل نسيجاً استراتيجياً مزدوج الأثر؛ فهي من جهة تمثل المادة الخام للابتكار وتخصيص الخدمات وخلق الميزة التنافسية، ومن جهة أخرى تجسد نقطة الضعف المركزية التي يمكن أن تعصف بسمعة المنظمة إذا ما نالت منها أيادي الاختراق. إن هذا التجاذب المستمر بين الحاجة الوجودية للانفتاح لتجميع البيانات، والضرورة القصوى للانغلاق لحمايتها، هو ما يمهد الطريق منطقياً لبحث الدور العملي والفعلي لهذه البيانات داخل المنظومة التسويقية، وهو ما سنعالجه في المبحث الموالي.

[1]– ميشيل ويتمان، هربرت ماتورد، مرجع سبق ذكره، ص 14.

المبحث الثاني: دور بيانات العملاء في التسويق الخدماتي

بعد أن أرسينا المعالم النظرية والحدود المفاهيمية لبيانات العملاء في المبحث السابق، تتجه بوصلة التحليل الآن نحو استجلاء الوظيفة العملية والطبيعة الديناميكية لهذه المعطيات داخل أروقة المنظمات الخدمية. إن المعرفة النظرية بخصائص البيانات تظل قاصرة وعقيمة إن لم تُربط مباشرة بالأثر التشغيلي الذي تحدثه في هندسة القرارات وسياسات التعامل مع السوق. فقد أحدثت الثورة المعلوماتية قطيعة نهائية مع أساليب الحدس والتخمين في الإدارة التسويقية، ليحل محلها نهج علمي صارم يستند حصرياً إلى مخرجات قواعد البيانات. وتتيح هذه القواعد للإدارة إمكانية الاستجابة الفورية للمتغيرات البيئية من خلال التنبؤ الاستباقي بسلوكيات الزبائن وصياغة استراتيجيات استهداف فائقة الدقة.[1]

يتجلى هذا الدور المحوري في مستويين متكاملين يعكسان صلب الفلسفة التسويقية الحديثة؛ يرتبط الأول بعملية "هندسة الخدمة" عبر تحليل التوقعات لتحسين الجودة المدركة وتخصيص العروض الترويجية بشكل فردي يلغي التباين بين ما يطلبه العميل وما يتلقاه. أما المستوى الثاني، فيتعلق بالتأسيس لعلاقة تبادلية مستدامة ومبنية على مبادئ الثقة والالتزام المؤسسي.[2]

غير أن هذا الاعتماد الكلي على الآثار الرقمية للمستهلكين يولد بيئة محفوفة بالتوتر، حيث يتقاطع السعي المحموم للمنظمة نحو التخصيص المطلق للخدمات مع تنامي ظاهرة "القلق الرقمي" لدى الزبائن خوفاً من انتهاك مساحاتهم الخاصة. هذا ما يحتم علينا في هذا المبحث تتبع دور البيانات في صناعة القرار وبناء العلاقة، ثم الوقوف وقفة نقدية صارمة أمام المخاطر القانونية، الأخلاقية، والمالية الكارثية التي تترتب على أي إخفاق في حماية هذه المعطيات أو التعسف في استخدامها، وهو الإخفاق الذي ينسف كل المكتسبات التسويقية ويقوض الثقة التي بُنيت بشق الأنفس.

المطلب الأول: أهمية بيانات العملاء في اتخاذ القرار التسويقي

تُعد عملية اتخاذ القرار التسويقي في بيئة الأعمال الخدمية المعاصرة من أعقد الممارسات الإدارية، نظراً للسمات الفريدة التي تتصف بها الخدمات كاللاملموسية، والتلازم بين التقديم والاستهلاك، وسرعة الزوال. وأمام هذه التحديات الهيكلية، تبرز بيانات العملاء كبوصلة استراتيجية وعصب حيوي يوجه مسار المنظمة وينتشلها من دائرة التخمين الإداري والعشوائية إلى فضاء اليقين العلمي والتوجيه الدقيق. لقد أحدث التدفق الهائل للمعلومات تغييراً جذرياً في هندسة القرارات، حيث لم يعد القرار وليد اللحظة أو نتاجاً لخبرة فردية متراكمة فحسب، بل أصبح يستند بشكل مكثف على القراءة التحليلية العميقة لملفات الزبائن وسلوكياتهم الرقمية. يتبلور هذا الدور الاستراتيجي لبيانات العملاء في مستويين متكاملين يصبان في

[1]– أليساندرو أكويستي وآخرون، مرجع سبق ذكره، ص 198.

[2]– بن مويزة أحمد، مرجع سبق ذكره، ص 296.

جوهر العملية التسويقية؛ يتعلق الأول بالهندسة العكسية للخدمة عبر تحسين جودتها وتطويرها المستمر لتلائم التوقعات، بينما ينصرف الثاني إلى الجانب التواصلي المتمثل في تخصيص العروض وتوجيه الحملات الترويجية بدقة متناهية.

أ. تحسين جودة الخدمات وتطويرها.

يقوم الفكر التسويقي الحديث على مسلمة أساسية مفادها أن العميل هو نقطة الانطلاق ونقطة الوصول في أي نشاط تجاري. وبناءً على ذلك، لا يمكن لأي منظمة خدمية أن تتخذ قراراً بتصميم خدمة جديدة أو إدخال تحسينات على خدمة قائمة بمعزل عن الفهم العميق والمجهري لاحتياجات سوقها المستهدف. هنا، تتدخل بيانات العملاء لتشكل المادة الخام الأولى التي تُبنى عليها بحوث التسويق والدراسات الاستطلاعية، مما يقضي على الكثير من المشكلات المتعلقة باستخدام أساليب بحوث التسويق التقليدية البطيئة والمكلفة. إن الاعتماد على قواعد البيانات يتيح لمتخذي القرار الحصول على المزيد من الأفكار والآراء بصفة لحظية ومستمرة، مما يساعد في دراسة مقترحات العملاء وشكاواهم لتعديل عناصر المزيج التسويقي وتصميم المنتجات وفقاً للرغبات الفردية.[1]

للتأصيل الأكاديمي لكيفية توظيف هذه البيانات في تطوير الخدمة، يمكن إسقاط هذا المسار على نموذج "آرثر دي ليتل (Arthur D. Little) "لدورة التسويق الإلكتروني، والذي يبرز دور المعلومات كمدخل حتمي في أولى مراحل القرار. يشير هذا النموذج إلى أن "مرحلة الإعداد (Preparation Phase)" تهدف جوهرياً إلى تحديد رغبات المستهلك وحاجاته، وتحديد الأسواق الجذابة وطبيعة المنافسة، ولا يتم اتخاذ أي قرار في هذه المرحلة إلا عن طريق الحصول على المعلومات والبيانات اللازمة التي تساعد المنظمة لاحقاً في طرح المنتجات والخدمات المناسبة.[2] إن غياب هذه البيانات أو تشوهها يعني اتخاذ قرارات تطويرية مبنية على فراغ، مما يؤدي إلى تصميم خدمات تفتقر إلى القيمة المدركة ولا تجد صدى لدى المستهلك النهائي.

تتجلى الخطورة الاستراتيجية لبيانات العملاء في قدرتها المباشرة على التحكم في مستويات "جودة الخدمة المدركة"، والتي تُعد المحرك الأساسي لرضا الزبون. فالرضا هو تقييم الزبائن لمنتج أو خدمة من جهة ما إذا كان هذا المنتج يلبي احتياجاتهم وتوقعاتهم ويشبعها.[3] ولفهم آلية هذا التقييم، نستند إلى النموذج الأمريكي لقياس رضا الزبون(ACIS) ، والذي يحدد ثلاثة عناصر تسبق حالة الرضا وتتحكم

[1]– العلاق بشير عباس، التسويق الإلكتروني، دار اليازوري العلمية للنشر والتوزيع، عمان، الأردن، 2010، ص 13.

[2]– العلاق بشير عباس ، التسويق الالكتروني، مرجع سبق ذكره، ص 11.

[3]– طويطي مصطفى، بوداود بومدين، نمذجة العلاقة السببية بين جودة الخدمة المدركة وقيمة الزبون بما يعزز رضاه إتجاه المؤسسة، مجلة الإستراتيجية والتنمية، العدد 15 مكرر، المجلد 08، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة مستغانم، 2018، ص 108 .

فيها: توقعات الزبون، الجودة المدركة، والقيمة المدركة. تلعب بيانات العملاء دور العصب الناقل في هذا النموذج؛ فمن خلال تحليل البيانات المستقاة من تقييمات العملاء السابقة وسجلات تفاعلاتهم، تستطيع الإدارة قياس "التوقعات" التي تشكلت لديهم قبل التجربة الاستهلاكية، وتستطيع تكييف أداء الخدمة الفعلي ليتطابق مع هذه التوقعات، مما يرفع من مستوى "الجودة المدركة" ويقلص الفجوة بين ما يتمناه العميل وما يتلقاه فعلياً.[1]

إلى جانب التطوير الاستباقي، تلعب بيانات العملاء المتمثلة في "سجلات الشكاوى والتذمر" دوراً تشخيصياً بالغ الأهمية في اتخاذ قرارات التحسين العلاجي. تُعد شكوى العميل من أهم العناصر التي تمكن المنظمة من قياس مستوى جودة الخدمة المقدمة وتحديد مكامن الخلل. إن تحليل قواعد البيانات التي ترصد هذه الشكاوى يكشف للإدارة عن المعايير التي يستخدمها العملاء لحكمهم على الجودة، وتساعد المنظمة في التغلب على المشاكل الخفية، وفي رسم السياسات التصحيحية الفورية لمنع تسرب الزبائن نحو المنافسين.[2]

تتجسد ذروة استغلال هذه المعطيات في عمليات "الإنتاج المشترك" للخدمة(Co-creation) ، حيث يتخذ المستهلك دوراً فاعلاً في صياغة ملامح الخدمة التي سيتلقاها. تشير الإحصائيات إلى نجاح العديد من المنظمات في إشراك العميل في إضافة المواصفات الخاصة بالمنتج الذي يبحث عنه استناداً إلى البيانات التي يطرحها طواعية عبر المنصات التفاعلية. هذا التدفق المعلوماتي اللحظي من العميل إلى المنظمة يحول عملية تطوير الخدمة من إجراء داخلي مغلق ومحفوف بالمخاطر، إلى استجابة مرنة ومضمونة العواقب، تضمن تقديم خدمة تتطابق تماماً مع المواصفات الفردية المطلوبة، وترفع من كفاءة الأداء التشغيلي وتقضي على الهدر في الموارد الناجم عن إنتاج خدمات غير مرغوبة.[3]

ب. تخصيص العروض والحملات التسويقية.

يُشكل الانتقال من نموذج "التسويق الشامل" إلى نموذج "التسويق الفردي" أو التسويق الموجه (One-to-One Marketing)إحدى أبرز ثمار الاستغلال العميق لبيانات العملاء في عملية اتخاذ القرار. في ظل الأسواق المتخمة بالرسائل الإعلانية والبدائل الخدمية، يفقد الترويج التقليدي غير الموجه فعاليته، وتصبح القدرة على لفت انتباه العميل مرتبطة بمدى شخصنة الرسالة التسويقية وملاءمتها لسياقه الزمني والنفسي. وتتخذ الإدارة التسويقية قراراتها الترويجية استناداً إلى الخصائص الديموغرافية، السلوكية، وتاريخ المشتروات المخزن في قواعد البيانات، لتقديم عروض مصممة على مقاس كل عميل بمفرده.

[1]– بوزيان حسان، أثر جودة الخدمات على رضا الزبون، مجلة الرؤى الإقتصادية، العدد 6، جامعة قسنطينة، 2014، ص 67.

[2]– عتيق خدجية، أثر المزيج التسويقي المصرفي على رضا العملاء، رسالة ماجستير، تخصص تسويق دولي، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة تلمسان، 2012، ص 146.

[3]– العلاق، بشير عباس ، التسويق الالكتروني، مرجع سبق ذكره، ص 14.

يظهر هذا التوجه التخصيصي جلياً في المجهودات التنظيرية التي حاولت إعادة صياغة عناصر المزيج التسويقي ليتلاءم مع البيئة الرقمية. فقد قدم الباحثان كاليانام وماكنتاير (Kalyanam & McIntyre)نموذجاً متطوراً لعناصر المزيج التسويقي الإلكتروني يُعرف بنموذج(P2C2S, 24) ، والذي يتجاوز العناصر الأربعة التقليدية ليضم عشرة عناصر أساسية تقود نجاح الأعمال الرقمية، من بينها: "التخصيص (Personalization) "و"الخصوصية (Privacy) "و"خدمات الزبون" و"المجتمعات الافتراضية".[1] إن إدراج "التخصيص" كعنصر مستقل وقائم بذاته في صلب المزيج التسويقي يعكس تحولاً جذرياً في الفكر الإداري؛ فالمنظمة لم تعد تكتفي بعرض خدمة نمطية، بل تستخدم الخوارزميات وقواعد البيانات لتحوير العرض، وتعديل السعر، وانتقاء قناة التواصل الأنسب لكل زبون بناءً على الأنماط المستخلصة من تفاعلاته السابقة.

تتعاظم الأهمية الاقتصادية لاتخاذ قرارات التخصيص عند النظر إلى كميات البيانات المجمعة كأصول استراتيجية ومولدات للربحية. تُجمع هذه البيانات، التي تشمل سمات الأفراد مثل الدخل، التفضيلات، ومسارات التصفح(Clickstream Data) ، لتشكل لوحة تحكم تتيح للمسوقين توجيه الخدمات، وتقديم إعلانات ذات صلة، أو حتى ممارسة استراتيجيات التمييز السعري[2]. من خلال تحليل هذه السجلات الرقمية، يكتسب متخذ القرار التسويقي قدرة استباقية (Predictive Analytics) تسمح له بالتنبؤ بالنوايا الشرائية للعميل قبل أن يُفصح عنها صراحة، مما يتيح تقديم حوافز تسويقية أو كوبونات خصم في اللحظة الحرجة التي تسبق اتخاذ قرار الشراء، وهو ما يرفع من معدلات التحويل (Conversion Rates)ويعظم العائد على الاستثمار في الحملات الترويجية.

إضافة إلى ذلك، تعتمد إدارة التسويق على أدوات التفاعل الإلكتروني كـ "البريد الإلكتروني الموجه" لبناء حوار مخصص ومستمر مع العميل. وتتركز وظيفة هذا الاتصال في إيصال الرسائل الترويجية المخصصة بناءً على سجل اهتمامات الزبون، وإشعاره بالمنتجات الجديدة التي تتوافق مع ذوقه.[3] هذا التفاعل المستند إلى البيانات يولد شعوراً بالاهتمام الشخصي لدى المستهلك الرقمي، ويُعرف هذا المستهلك بأنه الشخص الذي ينتقي ويشتري السلع والخدمات لاشباع حاجاته عن طريق التعاقد بالوسائل الإلكترونية، باحثاً عن تجربة فردية متميزة.[4]

[1]– العلاق، بشير عباس ، التسويق الالكتروني، مرجع سبق ذكره، ص 18

[2]– أليساندرو أكويستي وآخرون، مرجع سبق ذكره، ص 560.

[3]– العلاق، بشير عباس ، التسويق الالكتروني، مرجع سبق ذكره، ص 14.

[4]– –تهاني محمد عبد الرحمان فقيه، التسويق الالكتروني وأثره على إتجاهات الأسرة الإستهلاكية في عصر المعلوماتية، رسالة ماجستير، قسم السكن وإدارة المنزل، كلية التربية للإقتصاد المنزلي، جامعة أم القرى، السعودية، 2013، ص 69.

عندما يشعر هذا المستهلك أن العروض المقدمة تتناغم مع سلوكه ورغباته الدقيقة دون أن تمثل إزعاجاً عشوائياً، يتولد لديه التزام أعمق تجاه العلامة التجارية.

يتلاقى هذا الاستهداف الموجه مع مفاهيم "الإعلان السلوكي (Behavioral Targeting) " والتسويق الفيروسي. فالمنظمات الخدمية تقوم بجمع شتات البيانات التفاعلية والكلمة المنطوقة إلكترونياً لتحليل المزاج العام للعملاء داخل المجتمعات الافتراضية، ومن ثم بناء رسائل ترويجية شديدة الذكاء يسهل تداولها ومشاركتها بين المستهلكين بسرعة فائقة.[1] غير أن اتخاذ قرارات استهدافية فائقة الدقة يعمق من ظاهرة "التباين المعلوماتي" بين المنظمة والعميل، حيث تمتلك المنظمة رؤية شاملة وتفصيلية عن المستهلك، بينما يجهل الأخير الآلية التي عولجت بها بياناته لصياغة هذا العرض المخصص. هذا الخلل في التوازن يفرض تحدياً أمنياً وأخلاقياً خطيراً.[2]

إن فعالية تخصيص العروض ونجاح الحملات التسويقية الموجهة مرهونان جوهرياً بمدى استدامة تدفق هذه البيانات الدقيقة، وهو ما لا يمكن ضمانه إطلاقاً في بيئة رقمية هشة ومفتوحة للاختراقات ما لم تُحاط هذه القواعد بمنظومة أمن سيبراني صارمة. فإذا فقد العميل ثقته في قدرة المنظمة على حماية تفضيلاته وسجلاته الشرائية الحساسة من التسريب أو الاستغلال الخبيث، فإنه سيمتنع فوراً عن مشاركة هذه المدخلات، أو سيلجأ إلى تقنيات حجب التتبع، مما ينسف المادة الأساسية التي تُبنى عليها سياسات التخصيص، ويُعيد المنظمة إلى مربع التسويق العشوائي غير المجدي.

المطلب الثاني: بيانات العملاء وبناء العلاقة مع الزبون

شهدت الفلسفة التسويقية تحولاً هيكلياً عميقاً، متجاوزة الرؤية الكلاسيكية الضيقة التي كانت تحصر النشاط التجاري في مجرد إتمام صفقات بيعية منفصلة ومتقطعة، لتتبنى توجهاً استراتيجياً شاملاً يرتكز على بناء، تطوير، والمحافظة على تبادلات علائقية ناجحة وطويلة الأمد. هذا التحول الجذري، الذي يُعرف بأدبيات الإدارة بـ "التسويق بالعلاقات"، يعيد هندسة التفاعل بين مقدم الخدمة والمستهلك، جاعلاً من استمرارية الرابطة التفاعلية محوراً للتفوق التنافسي[3]. في قطاع الخدمات على وجه الخصوص، حيث تغيب الخصائص المادية الملموسة التي يمكن للزبون تقييمها قبل الشراء، تتحول "العلاقة" في حد ذاتها إلى بديل ملموس ومؤشر حاسم لتقييم جودة الخدمة المدركة. وتبرز بيانات العملاء في هذا النسق كحجر الأساس واللغة المشتركة التي تُبنى من خلالها هذه العلاقة؛ فلا يمكن لأي منظمة أن تدعي بناء علاقة شخصية مع زبون تجهل هويته، أو تفتقر إلى فهم دقيق لتاريخه الشرائي، وتفضيلاته، وتوقعاته المستقبلية.

[1]– العلاق، بشير عباس ، التسويق الالكتروني، مرجع سبق ذكره، ص 20

[2]– أليساندرو أكويستي وآخرون، مرجع سبق ذكره، ص 570

[3]– Robert M. Morgan, Shelby Hunt, The Commitment-Trust Theory of Relationship Marketing, J MARKETING, Jul 1994, p. 20.

يتطلب التأسيس لعلاقة حقيقية وذات معنى أن تمتلك المنظمة الخدمية فهماً مجهرياً للخصائص التكوينية والسلوكية لعملائها. وتلعب قواعد البيانات دور الجسر الإدراكي الذي يربط قدرات المنظمة بالحاجات الكامنة للزبون. من خلال الجمع المنهجي والتحليل المستمر للبيانات الديموغرافية، التفاعلية، وبيانات تدفق النقر، تتمكن إدارة التسويق من الانتقال من عقلية "السوق الشامل (Mass Market) "إلى استراتيجية "التسويق الفردي". يتيح هذا الفهم العميق تصميم حوار ثنائي الاتجاه، حيث يشعر العميل بأن المنظمة لا تخاطبه كعنصر نكرة ضمن شريحة واسعة، بل تتعامل معه ككيان مستقل ومتميز، مما يولد لديه شعوراً بالألفة والانتماء.[1]

تستند البنية التحتية لأي علاقة تسويقية مستدامة إلى ركيزتين سيكولوجيتين لا غنى عنهما: "الالتزام" و"الثقة". وتأخذ الثقة في بيئات الخدمة الرقمية أبعاداً شديدة الحساسية والتعقيد، إذ ترتبط ارتباطاً عضوياً بالكيفية التي تدير بها المنظمة الأصول المعلوماتية لعملائها.[2] تتفرع هذه الثقة إلى أبعاد جوهرية تتمثل أساساً في "الكفاءة (Competence) "و"النفع" أو حسن النية .(Benevolence) وتتجسد الكفاءة في قدرة المنظمة التقنية والتشغيلية على استخدام بيانات العميل لتقديم خدمة خالية من الأخطاء تتوافق تماماً مع رغباته. أما النفع، فيبرز عندما يدرك الزبون أن المنظمة تستخدم بصمته الرقمية وسجلاته الحساسة لغرض حصري يتمثل في تعزيز منفعته الشخصية وتسهيل حصوله على الخدمة، دون أن تسعى لاستغلال هذه المعطيات بشكل انتهازي أو بيعها لأطراف ثالثة دون علمه. عندما تنجح المنظمة في إثبات كفاءتها ونفعها عبر الإدارة الحكيمة للبيانات، يتطور لدى العميل التزام نفسي عميق يجعله مقاوماً لعروض المنافسين، ومستعداً للانخراط في علاقة طويلة الأجل.[3]

إن بناء الثقة يشكل دافعاً أساسياً يفوق في فاعليته مجرد محاولة تبديد مخاوف المستهلكين المتعلقة بالخصوصية. فقد أثبتت التجارب التسويقية أن العميل الذي يثق في العلامة التجارية يصبح أكثر انفتاحاً واستعداداً لتقديم معلوماته الشخصية طواعية[4].

---

[1]– Schoenbachler, D. D., Gordon, G. L., Trust and Customer Willingness to Provide Information in Database-Driven Relationship Marketing, Journal of Interactive Marketing, Number 3, Volume 16, 2002, p. 5.

[2]– بن مويزة أحمد، علاقة جودة الخدمة البنكية وجودة العلاقة عميل-بنك على رضا العملاء من خلال أبعاد الثقة والالتزام، مجلة العلوم الاقتصادية وعلوم التسيير، العدد 16، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة سطيف 1، الجزائر، 2016، ص 295.

[3]– فرحات، علاء الدين، "من الردع النووي إلى الردع السيبراني: دراسة لمدى تحقيق مبدأ الردع في الفضاء السيبراني"، مجلة المفكر، المجلد 16، جامعة محمد خيضر بسكرة، الجزائر، 2021.

[4]– Milne and Boza, Trust and concern in consumers' perceptions of marketing information management practices, Journal of Interactive Marketing, 1999, p. 5.

تنشأ هنا حلقة تفاعلية إيجابية(Positive Feedback Loop) ؛ فكلما زادت ثقة الزبون، قدم بيانات أكثر دقة وعمقاً للمنظمة، وبدورها، تستخدم المنظمة هذه البيانات العميقة لابتكار خدمات شديدة التخصيص تلبي أدق تطلعاته، وهو ما يؤدي بدوره إلى مضاعفة مستويات الثقة والرضا. هذا التبادل المتكافئ، حيث تمنح المنظمة "القيمة" مقابل "المعلومة"، يُعد جوهر الإدارة الحديثة لعلاقات العملاء (CRM)، ويمثل الميزة التنافسية الحقيقية التي يصعب على الشركات المنافسة استنساخها أو تقليدها.

يتجلى الاختبار الحقيقي لقوة العلاقة التسويقية في مرحلة ما بعد الشراء(After-Sales Phase) ، وهي المحطة الحرجة التي تحدد ما إذا كان الزبون سيتحول إلى عميل دائم أم أنه سيكتفي بتجربة عابرة. في هذا السياق، تؤكد النماذج التحليلية للتسويق الإلكتروني، كنموذج "آرثر دي ليتل"، أن المنظمات يجب ألا تتوقف جهودها عند إتمام عملية التبادل، بل يتعين عليها استغلال قواعد البيانات لتدعيم أواصر الولاء وتفعيل آليات التواصل المستمر. تقوم المنظمات بتوظيف البيانات السلوكية، مثل سجلات الشكاوى وتاريخ المشتريات، لإرسال رسائل بريدية مخصصة تحتوي على تحديثات أو نصائح استخدام تتطابق مع طبيعة الخدمة التي تلقاها العميل. علاوة على ذلك، يتيح تحليل البيانات دمج الزبائن ضمن مجتمعات افتراضية تفاعلية، حيث لا يقتصر التفاعل على مسار (منظمة–عميل)، بل يتسع ليشمل مسارات (عميل–عميل)، مما يخلق بيئة تشاركية تعزز من الانتماء العاطفي للعلامة التجارية وتجعل الزبون شريكاً فعلياً في تقييم وتطوير الخدمة. [1]

لضمان فاعلية هذه المرحلة، برزت الحاجة الماسة إلى تصميم وتفعيل برامج ولاء (Loyalty Programs)تعتمد جذرياً على التتبع الذكي لمعطيات الزبائن. إن تقديم مكافآت، نقاط، أو خصومات حصرية يتطلب بنية برمجية قادرة على رصد النشاط المتراكم للعميل ومكافأته بشكل عادل ولحظي. غير أن التحدي الأكبر يكمن في تصميم هذه البرامج بطريقة آمنة ومراعية للخصوصية، بحيث يتم تحقيق توازن دقيق بين الاحتفاظ بالعملاء (Customer Retention) وبين حماية أصولهم الرقمية من أي اختراق قد يحول برنامج الولاء من أداة لتعزيز العلاقة إلى ثغرة أمنية مدمرة[2].

على النقيض من هذه الديناميكية الإيجابية، فإن الاستغلال المكثف والعميق للبيانات الشخصية بغرض بناء العلاقات قد يولد، وبشكل مفارقاتي، ظاهرة سيكولوجية سلبية تُعرف بـ "قلق العميل " (Customer Anxiety)في البيئات الرقمية. إن الوعي المتزايد لدى المستهلكين بحجم البيانات التي يتم جمعها عنهم—من تتبع لمسارات التصفح، وتحليل للنقرات، ودمج للمعرفات الشخصية—يجعلهم في حالة

[1]– طويطي مصطفى وبوداود بومدين، مرجع سبق ذكره، ص 110.

[2] – Enzmann, M., Schneider, M., Improving Customer Retention in E–Commerce through a Secure and Privacy–Enhanced Loyalty System, Information Systems Frontiers, Number 4, Volume 7, 2005, p. 360.

ترقب وتوجس مستمرين. وعندما ترتفع مستويات هذا القلق، تتضرر جهود التسويق بالعلاقات بشكل بالغ، إذ يميل الزبائن إلى تبني سلوكيات دفاعية، مثل تقديم معلومات مغلوطة، أو استخدام تقنيات حجب التتبع، أو حتى الامتناع الكلي عن التفاعل مع المنصات الخدمية التي يراودهم الشك تجاه سياساتها الأمنية.[1]

لمواجهة هذا التحدي السيكولوجي، يقع على عاتق الإدارة التسويقية تبني سياسة "الشفافية التامة" كأداة لبناء العلاقة. فالمنظمة التي تُفصح لعملائها بوضوح عن ماهية البيانات التي تقوم بجمعها، والأغراض الاستراتيجية من وراء هذا الجمع، وكيفية حمايتها فنياً وقانونياً، تنجح في تخفيف حدة الإدراك بالمخاطر .(Perceived Risk) إن هذه الشفافية تُرسل رسالة ضمنية قوية للزبون باحترام استقلاليته وسيادته على بياناته الشخصية، مما يسهم بشكل فعال في تشكيل النوايا الشرائية المستقبلية وتعزيز الولاء الإلكتروني[2] .

يمتد الأثر الاستراتيجي للعلاقة القائمة على الاستخدام الآمن والفعال لبيانات العملاء ليتجاوز حدود التفاعل الثنائي، متسرباً بقوة إلى المحيط الشبكي الأوسع عبر ما يُعرف بالكلمة المنطوقة إلكترونياً .(eWOM)فالعميل الراضي، الذي يلمس احترام المنظمة لبياناته واستغلالها الدقيق لتقديم خدمة متفوقة وتجربة استهلاكية خالية من الاحتكاك، يتحول تدريجياً إلى مدافع ومروج مجاني للعلامة التجارية. إن هذا العميل يميل إلى مشاركة تقييماته الإيجابية، ومراجعاته، وتوصياته عبر المنتديات وشبكات التواصل الاجتماعي، وهو ما يعزز السمعة الرقمية للمؤسسة ويجذب شرائح جديدة من الزبائن الذين يعتمدون بشكل مكثف على آراء نظرائهم لتخفيض حالة عدم التأكد المرتبطة بالخدمات اللاملموسة.[3] يفرض هذا المشهد التشغيلي المعقد ضرورة إقرار حقيقة استراتيجية مفادها أن توظيف وسائط الاتصال الحديثة والبيانات الضخمة لخلق علاقات تفاعلية يشكل تحدياً هائلاً لإدارة التسويق [4].لم يعد النجاح التسويقي يقاس فقط بقدرة الخوارزميات على تصنيف البيانات وتقديم العروض المخصصة، بل بات مرهوناً بالقدرة على إدماج "الأمن والموثوقية" كعناصر محورية في صلب المزيج التسويقي الموجه لبناء العلاقات. فكل تفاعل رقمي، وكل رسالة موجهة، وكل استرجاع لتفضيل سابق، يمر عبر قنوات تكنولوجية يجب أن تكون محصنة ضد التهديدات.

---

[1]– Khoa, B. T., Huỳnh, T. T., How do customer anxiety levels impact relationship marketing in electronic commerce?, Cogent Business & Management, Number 1, Volume 9, 2022, p. 5.

[2]– Ha, N. T., The effect of trust on consumers' online purchase intention: An integration of TAM and TPB, Management Science Letters, 2019, p. 1451.

[3]– كريستيان تشيونغ وآخرون، مرجع سبق ذكره، ص 233.

[4]– Stauss, B., Using new media for customer interaction: a challenge for relationship marketing, in Relationship Marketing, Springer, 2000, p. 28.

نخلص من هذا الطرح التحليلي إلى أن بيانات العملاء تمثل الدورة الدموية التي تغذي العلاقة بين المنظمة الخدمية والزبون. إنها تمنح الخدمة روحاً شخصية، وتحول المستهلك من رقم عابر في سجلات المحاسبة إلى شريك استراتيجي طويل الأمد. غير أن هذه الدورة الدموية محكومة بثنائية الثقة والقلق؛ فبقدر ما تساهم دقة البيانات في تعميق الالتزام وتحقيق رضا العميل[1] ، بقدر ما يشكل أي تسريب أو انتهاك لخصوصية هذه المعطيات ضربة قاصمة تنهي العلاقة بشكل فوري وتدمر الثقة المكتسبة بصورة لا رجعة فيها[2]. هذا التناقض الحرج هو ما يدفعنا منطقياً، في خطوتنا التحليلية القادمة، إلى تفكيك وفحص التداعيات الخطيرة والمخاطر المترتبة عن سوء استغلال هذه البيانات أو فقدانها، وانعكاسات ذلك على الكيان التسويقي للمؤسسة.

المطلب الثالث: مخاطر سوء استغلال بيانات العملاء وانعكاساته التسويقية

تتعامل المنظمات الخدمية المعاصرة مع بيانات العملاء بوصفها سيفاً ذا حدين؛ ففي حين تمثل هذه المعطيات المحرك الأساسي لخلق الميزة التنافسية وتخصيص الخدمات، فإن أي اختراق أو سوء استغلال لها يحولها فوراً إلى مصدر تهديد وجودي يعصف بكيان المؤسسة. إن تجميع الكتل الضخمة من البيانات الشخصية والحساسة يجعل من المنظمات أهدافاً مغرية للتهديدات في الفضاء الرقمي، حيث أن فقدان هذه البيانات لا يمثل مجرد خسارة تقنية عابرة، بل هو انهيار مباشر لمقومات الاستراتيجية التسويقية[3]. ويتجاوز مفهوم "سوء الاستغلال" مجرد التعرض للاختراق من قبل قراصنة خارجيين، ليمتد ليشمل الممارسات التسويقية التعسفية داخل المنظمة ذاتها، كجمع البيانات دون موافقة، أو استخدامها في أغراض تتنافى مع ما تم التصريح به للعميل. تتفرع التداعيات العميقة لهذا الانكشاف الرقمي وسوء الاستغلال إلى ثلاثة أبعاد استراتيجية متداخلة.

أولاً: المخاطر القانونية والأخلاقية

لقد أفرز التطور المتسارع في تقنيات جمع وتحليل البيانات فراغاً تشريعياً في بدايات الثورة الرقمية، غير أن تصاعد وتيرة الانتهاكات دفع الحكومات والهيئات الدولية إلى صياغة ترسانة قانونية صارمة تضع قيوداً حازمة على آليات المعالجة التسويقية. وتواجه المنظمات اليوم مخاطر قانونية جسيمة في حال إخفاقها في توفير الحماية السيبرانية لعملائها أو عند انتهاكها لمبادئ الخصوصية. فعلى سبيل المثال، يفرض المشرع عقوبات إدارية وجزائية قاسية على المؤسسات التي تفشل في تأمين أنظمتها، حيث تتضمن التشريعات الحديثة، كقانون حماية البيانات الشخصية السعودي(PDPL) ، غرامات مالية ضخمة

[1]– طويطي مصطفى، بوداود بومدين، مرجع سبق ذكره، ص 115.

[2]– Strzelecki, A., Rizun, M., Consumers' Change in Trust and Security after a Personal Data Breach in Online Shopping, Sustainability, Number 10, Volume 14, 2022, p. 5866.

[3]–نوفيل حديد، كربيط حنان، مرجع سبق ذكره، ص 50.

تصل إلى 5 ملايين ريال سعودي لكل انتهاك، وتتضاعف في حالة المخالفات المتكررة، لتصل إلى عقوبات بالسجن في حالات خرق البيانات الجسيمة المتمثلة في نشر بيانات حساسة دون موافقة أصحابها.[1]

يمتد هذا التوجه التشريعي الصارم ليشمل مختلف البيئات القانونية، بما فيها البيئة الجزائرية التي سعت لسد الثغرات عبر قوانين متخصصة كالقانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي. يفرض هذا الإطار القانوني على متخذي القرار التسويقي الالتزام بمبادئ الموافقة المسبقة، وضمان أمن الأنظمة المعلوماتية، تحت طائلة تعرض المؤسسة لمساءلات قانونية قد تصل إلى حد تعليق أنشطتها أو توقيع عقوبات مشددة على مسيريها في حال ثبوت الإهمال في حماية تلك القواعد الحساسة.[2]

بموازاة المخاطر القانونية، تبرز المخاطر الأخلاقية كعنصر أشد تعقيداً في مسار العلاقة التسويقية. فالالتزام الأخلاقي يتجاوز مجرد الامتثال للنصوص القانونية الجافة، ليلامس جوهر العقد النفسي المبرم بين المنظمة والزبون. وتنشأ الإشكالية الأخلاقية عندما تقوم الإدارة التسويقية بممارسة ما يُعرف بـ "الاستخدام الثانوي (Secondary Usage) "للبيانات. يحدث هذا عندما يوافق المستهلك طواعية على تقديم معلوماته لغرض إتمام خدمة محددة، ليُفاجأ لاحقاً بأن المنظمة قامت ببيع أو مشاركة تلك البيانات مع أطراف ثالثة أو استخدمتها لتوجيه إعلانات سلوكية تتدخل في أدق تفاصيل حياته دون علمه المسبق.[3]

إن هذا السلوك الانتهازي يعمق من ظاهرة "التباين المعلوماتي" بين البائع والمشتري، حيث تمتلك المنظمة رؤية مجهرية حول المستهلك، بينما يجهل الأخير الكيفية التي تُعالج بها بياناته.[4] يؤدي هذا الخلل الأخلاقي إلى شعور العميل بالانتهاك والاستغلال، فالمستهلك الرقمي المعاصر يمتلك وعياً متزايداً بقيمة بصمته الرقمية، وأي محاولة لتضليله أو استغلال ثغرته المعرفية تنعكس فوراً في شكل ردود فعل عكسية تدمر مساعي بناء الولاء. ويضاف إلى ذلك المعضلة الأخلاقية المتعلقة بمدى شفافية المنظمة في الإفصاح عن الاختراقات؛ إذ تميل بعض الشركات إلى التكتم على حوادث تسريب البيانات خوفاً من الإضرار بسمعتها، وهو ما يمثل خيانة صريحة لأمانة المستهلك ويحرمه من اتخاذ التدابير الوقائية

[1]- Resecurity. n.d.. PDPL Compliance in Saudi Arabia. Resecurity. Retrieved from https://www.resecurity.com/compliance/pdpl-saudi-arabi

[2]- مقدر نبيل، جهود الجزائر في تحقيق الأمن السيبراني، مجلة مجمع، العدد 22، المجلد 62، جامعة المدينة العالمية، ماليزيا، 2018، ص 326.

[3]- أليساندرو أكويستي وآخرون، مرجع سبق ذكره، ص 565

[4]- المرجع السابق، ص 194.

اللازمة لحماية حساباته، مما يضاعف من حجم الضرر اللاحق به ويوقع المؤسسة في طائلة التواطؤ الأخلاقي.

ثانياً: فقدان الثقة وتضرر السمعة المؤسسية

في اقتصاد الخدمات الذي يتسم باللاملموسية، تمثل الثقة رأس المال الحقيقي للمنظمة وأهم أصولها غير الملموسة. وتُبنى هذه الثقة عبر تراكم التفاعلات الإيجابية وتأكد العميل من قدرة المنظمة على الإيفاء بوعودها، وفي مقدمتها وعد "الموثوقية والأمان". غير أن حوادث خرق البيانات وسوء استغلالها تنسف هذا التراكم بشكل لحظي ودرامي. إن تسريب السجلات الشخصية أو المالية للزبائن يوجه رسالة ضمنية قاطعة مفادها أن المؤسسة تفتقر إلى الكفاءة التشغيلية ولا تحترم وعودها السرية، مما ينقل العميل من حالة "الرضا" إلى حالة من "التشكيك المفرط" في كافة عمليات المنظمة[1]

تؤكد الدراسات السلوكية الحديثة عمق هذا الأثر السيكولوجي، حيث تشير الإحصائيات إلى أن تداعيات اختراق البيانات تمتد لتغيير الأنماط الاستهلاكية للمتضررين بشكل جذري. فقد صرح حوالي 65% من المستهلكين الذين تعرضت بياناتهم للانتهاك بأنهم فقدوا الثقة تماماً في الشركات المعنية، مما يؤدي إلى تراجع فوري في مستويات التفاعل وتقليص الرغبة في مشاركة أي معطيات مستقبلية.[2] وفي سياق متصل، كشفت بحوث متخصصة أن شريحة واسعة من المستهلكين أصبحت أكثر صرامة في قراراتها، حيث أفاد 70% من الأفراد بأنهم سيتوقفون نهائياً عن التسوق أو التعامل مع العلامة التجارية التي تتعرض لحادث أمني يؤدي إلى كشف بياناتهم[3]

لا يتوقف هذا النزيف عند حدود العميل المتضرر فحسب، بل يتمدد كالنار في الهشيم بفضل آليات "الكلمة المنطوقة إلكترونياً (eWOM) "السلبية. ففي بيئات التواصل الاجتماعي والمنتديات المفتوحة، يميل المستهلكون المحبطون إلى تضخيم تجاربهم ومشاركتها بشكل مكثف للتحذير من التعامل مع المنظمة المخترقة. وتشير التقديرات إلى أن 85% من المستهلكين يشاركون تجاربهم السيئة المتعلقة بالأمن الرقمي مع الآخرين، وهو ما يلحق أضراراً بالغة ومستدامة بالسمعة المؤسسية[4]

---

[1]- Singh, H., Anand, N., Singh, S., Angirish, N., Sengupta, P. D., & Amin, S. 2025. Examining the Impact of personal Data Breaches on Consumer Trust and Privacy Protection Behavior in E-Commerce. Advances in Consumer Research, 25, 2101.

[2]- المرجع السابق، ص 2104.

[3] -Vercara. 2024. New Vercara Research Reveals Impact of Trust in Brands Following Breaches, Concerns Around Outside Threats. Vercara. Retrieved from https://vercara.digicert.com/news/new-vercara-research-reveals-impact-of-trust-in-brands-following-breaches-concerns-around-outside-threats.

[4]- Brand Reputation &Hardeep singh, opcit, p2101.

تصبح العلامة التجارية في أذهان الجمهور مقترنة بمفاهيم "الهشاشة" و"الإهمال"، مما يحيد مفعول الملايين التي تُصرف على الحملات الإعلانية الترويجية.

تفرض هذه الأزمة السمعية على المؤسسة الدخول في نفق مظلم من محاولات ترميم الصورة الذهنية. وتجد الإدارة التسويقية نفسها مجبرة على التخلي عن استراتيجيات التوسع واكتساب عملاء جدد، لتوجيه كافة ميزانياتها وجهودها نحو إدارة الأزمة (Crisis Management) ومحاولة إقناع السوق بأنها اتخذت تدابير تصحيحية. ومع ذلك، فإن ذاكرة المستهلك الرقمي تتسم بالطول والحذر، والشركات التي تفشل في معالجة تداعيات الخرق بشفافية وسرعة تعاني من انخفاض حاد في ولاء الزبائن (Customer Loyalty)، وتصبح عاجزة عن استقطاب شرائح جديدة تضع معيار "الأمن السيبراني" على رأس أولوياتها عند تقييم البدائل الخدمية المتاحة.

ثالثاً: الخسائر المالية وتراجع الحصة السوقية

تشكل التبعات القانونية والانهيار السمعي الناجم عن سوء استغلال بيانات العملاء تمهيداً حتمياً لكارثة اقتصادية متكاملة الأركان تضرب الميزانية العامة للمؤسسة. إن التكلفة المالية المترتبة على الهجمات السيبرانية أو تسريب البيانات لا تقتصر على النفقات الفورية لتصليح الأنظمة، بل تتفرع إلى شبكة معقدة من التكاليف المباشرة وغير المباشرة التي تستنزف الموارد. وقد أثبتت التقارير العالمية المتخصصة مدى فداحة هذه التكلفة، حيث بلغ المتوسط العالمي للتكلفة الإجمالية لخرق البيانات الواحد حوالي 4.35 مليون دولار أمريكي، في حين ترتفع هذه التكلفة لتصل إلى 4.82 مليون دولار للمنظمات العاملة في قطاعات البنية التحتية الحساسة كالخدمات المالية والصحية.[1]

تتوزع هذه الخسائر المالية الضخمة على عدة فئات تشغيلية تعيق نمو المنظمة. في المرحلة الأولى، تتكبد المؤسسة التكاليف المباشرة التي تشمل الاستعانة بخبراء التحقيق الجنائي الرقمي (Forensic Experts)لتحديد حجم الاختراق، ونفقات إخطار العملاء المتضررين، وتخصيص مراكز اتصال للرد على استفساراتهم، بالإضافة إلى التسويات القانونية المحتملة والغرامات التنظيمية.[2] علاوة على ذلك، تواجه الإدارة تكاليف باهظة لإعادة تأهيل البنية التحتية التكنولوجية المعطوبة واسترجاع البيانات المفقودة، وهو ما يمثل ضغطاً استثنائياً على الميزانية المخصصة للتطوير والابتكار.

غير أن الخطر الأكبر، والذي يقع في صميم العمل التسويقي، يتجسد في التكاليف غير المباشرة المرتبطة بـ "خسارة الأعمال .(Lost Business) "لقد أظهرت التحليلات أن فئة خسارة الأعمال تُعد من

[1] –IBM Security. 2022. Cost of a Data Breach Report 2022. IBM Corporation. p. 4.

[2] – المرجع السابق، ص 18.

أضخم مكونات تكلفة خرق البيانات، حيث تتجاوز 1.42 مليون دولار من إجمالي التكلفة[1]. وتتضمن هذه الفئة الخسائر الناجمة عن تعطل الأنظمة وتوقف تقديم الخدمة لفترات زمنية، وما يصاحب ذلك من ضياع لفرص بيعية محققة. والأهم من ذلك، تشمل هذه التكلفة "تسرب الزبائن (Customer Churn) " نحو المنافسين نتيجة فقدان الثقة، وما يترتب عليه من ضرورة مضاعفة الإنفاق على حملات اكتساب عملاء جدد (CAC) لتعويض النزيف الحاصل في قاعدة الزبائن الحالية.[2] تنعكس هذه السلسلة من الخسائر المالية والتسرب في قاعدة العملاء بشكل هندسي على "الحصة السوقية (Market Share) " للمؤسسة. في ظل بيئة شديدة التنافسية، يمثل الانكشاف الأمني لإحدى المنظمات فرصة ذهبية للمنافسين الذين يمتلكون سجلات أمنية نظيفة لافتراس حصتها السوقية والترويج لأنفسهم كملاذات آمنة وموثوقة. ومع تآكل القيمة المدركة للعلامة التجارية، تجد المؤسسة المخترقة نفسها مضطرة لتقديم تنازلات سعرية حادة أو خصومات غير مبررة اقتصادياً في محاولة يائسة للاحتفاظ بما تبقى من عملائها، وهو ما يؤدي إلى تآكل هوامش الربحية وتراجع العائد على الاستثمار.

على المستوى الماكرو–اقتصادي، يحمل هذا الفشل في توفير الحماية عواقب وخيمة على الاقتصاد الرقمي برمته. إذ تقدر التقارير الاقتصادية أن المؤسسات تخاطر بفقدان حوالي 5.2 تريليون دولار أمريكي من فرص خلق القيمة في الاقتصاد الرقمي خلال السنوات القادمة كنتيجة مباشرة للتهديدات السيبرانية وعجز الأنظمة عن احتواء سوء استغلال البيانات[3].

تأسيساً على هذا التحليل، يبرز الاستنتاج المحوري بأن إهمال التدابير الأمنية لم يعد مجرد خطأ تقني داخلي، بل هو انتحار تسويقي استراتيجي. إن البيانات التي تُجمع لتكون أداة للنمو وتخصيص العروض، تنقلب لتصبح الأداة التي تقوض الميزة التنافسية وتدفع بالمؤسسة خارج دائرة السوق إذا ما افتقرت إلى الغطاء السيبراني المنيع. وهو ما يمهد الطريق منطقياً للانتقال نحو دراسة الجانب الوقائي المتمثل في ماهية الأمن السيبراني وأدواره الفعلية في صد هذه الانعكاسات، والذي سيمثل محور نقاشنا في الفصل الثاني من هذه المذكرة.

[1]– المرجع السابق، ص 7

[2] –OECD. 2019. Measuring Digital Security Risk Management Practices in Businesses OECD Digital Economy Papers, No. 283. OECD Publishing, Paris. p. 18.

[3]– Abbosh, O., & Bissell, K. 2019. Securing the Digital Economy: Reinventing the Internet for Trust. Accenture. p. 16.

خلاصة الفصل الأول

نخلص من خلال التحليل المعمق والمستفيض لمسارات هذا الفصل إلى حقيقة مركزية لا تقبل الجدل، وهي أن "بيانات العملاء" قد تجاوزت دورها التقليدي كأرشيف للإدارة أو مجرد سجلات لتوثيق العمليات المحاسبية، لتتربع على عرش الأصول الاستراتيجية المنتجة للقيمة في قطاع التسويق الخدماتي المعاصر. لقد أفرزت تكنولوجيا المعلومات والاتصالات بيئة خصبة مكنت المنظمات من رصد، وتتبع، وتحليل البصمة الرقمية للمستهلكين بدرجة مجهرية من الدقة. هذا التدفق المعلوماتي، سواء في شقه الديموغرافي أو السلوكي التفاعلي، أحدث ثورة في آلية اتخاذ القرار، مانحاً الإدارة التسويقية قدرات تنبؤية فائقة سمحت لها بالانتقال بسلاسة نحو تبني نماذج التسويق الفردي الموجه، وتصميم خدمات مخصصة تخاطب الاحتياجات الكامنة لكل زبون وتستجيب لتوقعاته اللحظية.

تتضح لنا قوة هذه المعطيات في قدرتها الفائقة على خلق رابطة عضوية بين المنظمة والعميل، حيث تمثل البيانات لغة الحوار الصامتة التي تبني صروح "التسويق بالعلاقات". إن استشعار الزبون بأن المنظمة تستغل سجلاته الشرائية لغرض وحيد وهو تعزيز منفعته الشخصية وتسهيل حصوله على الخدمة، يرفع من مستويات الرضا لديه، ويولد التزاماً سيكولوجياً يخفض من احتمالية تسربه نحو المنافسين، ما يكرس مبدأ الثقة كأهم أصل غير ملموس يضمن استدامة المردودية الاقتصادية.

بيد أن هذا المشهد التسويقي المثالي يخبئ في طياته جانباً مظلماً وبالغ الخطورة. فالدراسة التحليلية لخصائص هذه البيانات أوضحت هشاشتها المتأصلة؛ إذ إن طبيعتها اللاملموسة، وقابليتها للاستنساخ، وحساسيتها الفائقة الناتجة عن تجميعها التراكمي، تجعلها الغنيمة الأبرز في الفضاء الافتراضي. إن تحول المؤسسة إلى مستودع مركزي لأسرار العملاء وتوجهاتهم المالية والاجتماعية يضعها تحت مجهر التهديدات والقرصنة. وهنا تتبدد كل الجهود التسويقية إذا ما تعرضت المنظمة لأي خرق استنزافي. فسوء الاستغلال، سواء كان داخلياً بانتهاك أخلاقيات الخصوصية، أو خارجياً عبر هجمات سيبرانية، يؤدي بشكل فوري إلى نتائج تدميرية مركبة، تبتدئ بالمساءلات القانونية الصارمة، وتمر عبر انهيار السمعة المؤسسية وفقدان ثقة الجمهور (والتي تنشرها بسرعة آليات الكلمة المنطوقة إلكترونياً السلبية)، لتنتهي بخسائر مالية فادحة وتقلص حاد في الحصة السوقية.

إن هذا الاستنتاج الحرج يضع متخذي القرار أمام حتمية مفادها أن الفلسفة التسويقية التوسعية في جمع البيانات لا يمكن أن تنجح أو تستدام في فراغ أمني. لم تعد جودة الخدمة وحدها تكفي لخلق الولاء، بل أصبحت "الموثوقية الرقمية" والقدرة على تأمين الأنظمة شرطاً أساسياً وجزءاً لا يتجزأ من المزيج التسويقي. إن الملايين التي تُستثمر في حملات الترويج وإدارة علاقات العملاء ستذهب أدراج الرياح إن لم تقترن بدرع واقٍ يصد التهديدات ويحفظ قدسية البيانات.

من هذا المنطلق، وبالنظر إلى هذا التلازم العضوي بين التسويق والحماية، تبرز الحاجة الماسة والمنطقية للانتقال من دراسة طبيعة البيانات وخصائصها، إلى استكشاف الآليات الفعلية القادرة على توفير هذه البيئة الآمنة، وهو ما يمهد الطريق أمامنا للخوض في غمار "الفصل الثاني"، والذي سيُخصص بالكامل لمعالجة مفهوم، وهيكلة، واستراتيجيات "الأمن السيبراني" كأداة حتمية لضمان استمرارية النشاط التسويقي، والحفاظ على بيانات العملاء في بيئة الأعمال الجزائرية والدولية.

الفصل الثاني:

الأمن السيبراني وحماية بيانات العملاء

أفرزت التحولات العميقة التي تناولناها في الفصل الأول حقيقة اقتصادية وتسويقية حتمية، تتمثل في انتقال بيانات العملاء من مجرد أرشيف إداري جامد إلى أصول استراتيجية ومولدات حقيقية للقيمة والميزة التنافسية. غير أن هذا الاعتماد الجذري على البصمة الرقمية للمستهلك وتجميعها المكثف داخل خوادم المؤسسات الخدمية، لم يأتِ دون ثمن، بل ألقى بهذه الكيانات في خضم بيئة افتراضية شديدة العدائية ومفتوحة على مختلف أشكال الاختراق والقرصنة. إن هذا الانكشاف الاستراتيجي يفرض على الإدارة الحديثة تجاوز عقلية التسويق التوسعي البحت، ليصبح لزاماً عليها هندسة جدران دفاعية تحمي هذه المكتسبات، وهو ما ينقلنا مباشرة من حقل التسويق الخدماتي إلى النطاق التقني والقانوني المتمثل في الأمن السيبراني.

يعتبر تبني تدابير الحماية السيبرانية في الوقت الراهن التزاماً قانونياً وضرورة بقاء، وليس مجرد خيار تكنولوجي تكميلي. فالمؤسسة التي تفشل في تأمين قواعد بياناتها تفقد فوراً ثقة عملائها وتتعرض لمساءلات تشريعية صارمة تعصف بكيانها. تأسيساً على هذا التلازم العضوي بين القيمة التسويقية للمعلومة وضرورة حمايتها، يخصص هذا الفصل للغوص في أعماق الأمن السيبراني كمنظومة دفاعية متكاملة. سنعالج في المبحث الأول التأصيل النظري والمفاهيمي لهذا الوافد الجديد على الفكر الإداري، لننتقل في المبحث الثاني إلى قياس فعالية آلياته وتأثيرها المباشر في تعزيز ثقة العملاء وحماية بياناتهم ضمن بيئة الأعمال المعاصرة.

المبحث الأول: الإطار النظري للأمن السيبراني

يقتضي البحث الأكاديمي الرصين قبل الخوض في الآليات التشغيلية والفعالية التطبيقية لأي ظاهرة، بناء أرضية إبستمولوجية صلبة تفكك مصطلحاتها وتحدد إطارها النظري بدقة. إن الأمن السيبراني يمثل حقلاً معرفياً حديث النشأة وشديد التعقيد، تتقاطع فيه علوم الحاسوب مع الإدارة، والقانون، والسياسات الأمنية. هذا التداخل يفرض علينا تتبع الجذور التاريخية واللغوية للمصطلح، لفهم كيف تطورت النظرة إلى حماية الفضاء الافتراضي من مجرد إجراءات تقنية معزولة إلى عقيدة دفاعية شاملة تتبناها الدول والمؤسسات لحماية أصولها الحيوية.

لا يستقيم هذا التحليل دون إزالة اللبس المفاهيمي القائم بين الأمن السيبراني والمصطلحات الرديفة التي سبقته تاريخياً، وعلى رأسها أمن المعلومات، حيث تختلف النطاقات وتتباين طبيعة التهديدات التي يعالجها كل حقل. وانطلاقاً من هذا المسار المنهجي، سيتناول هذا المبحث في مطلبه الأول مفهوم الأمن السيبراني وتطوره التاريخي مع التمييز بينه وبين أمن المعلومات، لنتطرق في المطلب الثاني إلى الأهداف الاستراتيجية التي تسعى المؤسسات لتحقيقها من خلاله، وصولاً إلى المطلب الثالث الذي سيفصل في المبادئ الأمنية المركزية المرتبطة ارتباطاً وثيقاً بضمان قدسية بيانات العملاء.

المطلب الأول: مفهوم الأمن السيبراني

يستوجب البحث الأكاديمي الرصين قبل الولوج في الآليات التشغيلية والفعالية التطبيقية لأي ظاهرة تكنولوجية، بناء أرضية صلبة تفكك مصطلحاتها وتحدد إطارها النظري والقانوني. يمثل الأمن السيبراني حقلا معرفيا متشابكا تتقاطع فيه علوم الحاسوب مع الإدارة والقانون والسياسات الأمنية. هذا التداخل المعقد يفرض تتبع الجذور التاريخية واللغوية للمصطلح لفهم تطور النظرة إلى حماية الفضاء الافتراضي من مجرد إجراءات تقنية معزولة، إلى عقيدة دفاعية شاملة تتبناها المؤسسات الخدمية لحماية أصولها وبيانات عملائها. لا يستقيم هذا التحليل دون إزالة اللبس المفاهيمي القائم بين الأمن السيبراني والمصطلحات الرديفة التي سبقته تاريخيا وعلى رأسها أمن المعلومات، حيث تختلف النطاقات وتتباين طبيعة التهديدات التي يعالجها كل حقل.

أولاً: التطور التاريخي والمفهوم العام

ترتبط المفاهيم المعاصرة بالسياقات الزمنية والتقنية التي أفرزتها، ولا يشذ الأمن السيبراني عن هذه القاعدة، إذ يمثل استجابة حتمية لتطور بيئة الاتصالات وانتقال المجتمعات نحو الاعتماد الكلي على الفضاء الرقمي المفتوح. بالرجوع إلى الجذور اللغوية نجد أن المصطلح يتكون من شقين، الأول هو الأمن والذي يعبر في دلالاته اللغوية عن الطمأنينة والسلم ونقيض الخوف، في حين يمثل الشق الثاني سيبراني

تعريبا للكلمة الإنجليزية التي تعود في أصلها اللغوي إلى الكلمة اليونانية القديمة التي كانت تستخدم للدلالة على الشخص الذي يدير دفة السفينة أو المتحكم في مسارها.[1]

تاريخيا ينسب التوثيق الأكاديمي ظهور هذا المصطلح في سياقه العلمي إلى عالم الرياضيات الأمريكي نوربرت وينر خلال أواخر أربعينيات القرن الماضي، حيث استخدم مصطلح السيبرانية للتعبير عن آليات التحكم والتوجيه الآلي في الأنظمة المعقدة وعلم الضبط. ومع تحول هذه الأنظمة الآلية إلى شبكات حاسوبية مترابطة، تطور مفهوم التحكم ليأخذ أبعادا دفاعية خالصة.

يعود الانتباه الفعلي لحتمية بناء جدران حماية سيبرانية إلى حقبة الثمانينيات التي شهدت أولى الهجمات التخريبية واسعة النطاق، لعل أبرزها حادثة أنبوب النفط السيبيري وما تلاها من ظهور البرمجيات الخبيثة كدودة موريس، وهو ما أعلن رسميا نهاية حقبة الأمن المادي البحت وبداية عصر الصراعات الافتراضية التي تستهدف البنى التحتية المعلوماتية وتتطلب تدخلات وقائية صارمة تتجاوز الحلول التقليدية.[2]

من الزاوية الاصطلاحية تعددت المقاربات التي حاولت تأطير هذا المفهوم نظرا لتعدد الفواعل المتدخلة في الفضاء الرقمي وطبيعة المصالح المحمية. قدم الاتحاد الدولي للاتصالات مقاربة تقنية وتنظيمية موسعة حيث عرف الأمن السيبراني بأنه مجموعة من الأدوات والسياسات ومفاهيم الأمن والضمانات الأمنية والمبادئ التوجيهية وإدارة المخاطر والتدريب وأفضل الممارسات التي يمكن استخدامها لحماية البيئة الإلكترونية وتنظيم أصول المؤسسات والمستخدمين. يركز هذا الطرح على الطابع الشمولي للأمن والذي لا يكتفي بالبرمجيات المضادة بل يمتد ليشمل العنصر البشري وتدريبه كخط دفاع أساسي ضد الاختراقات التي تستهدف قواعد البيانات الحساسة.[3]

في ذات السياق التنظيمي تبنت الجهات السيادية مقاربات تركز على القدرة على الصمود وردع التهديدات. فقد عرفت وزارة الدفاع الأمريكية الأمن السيبراني بأنه جميع الإجراءات التنظيمية والتقنية التي تتخذ لضمان الحماية الكافية للمعلومات بجميع أنواعها وأشكالها المادية والإلكترونية من مختلف المخاطر والهجمات كالتخريب والتجسس، في حين يرى الإعلان الأوروبي أن جوهر هذا الأمن يكمن في قدرة النظام المعلوماتي على مقاومة محاولات الاختراق غير المتوقعة التي تستهدف البيانات أو البنى التحتية وتؤدي إلى تسريبها للعلن. تبرز هذه التعاريف تحولا استراتيجيا في الفكر الإداري والأمني حيث لم يعد

[1] منى عبد الله السمحان، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية، العدد 111، جامعة المنصورة، المملكة العربية السعودية، 2020، ص 9.

[2] أويس مجيد غالب العوادي، الأمن السيبراني المعلوماتي، سلسلة إصدار مركز الدراسات والتخطيط، العراق، 2016، ص 4.

[3] ليلى بن برغوث، الأمن السيبراني وحماية خصوصية البيانات الرقمية في الجزائر في عصر التحول الرقمي والذكاء الاصطناعي، المجلة الدولية للاتصال الاجتماعي، العدد 21، المجلد 12، جامعة عبد الحميد بن باديس مستغانم، 2020، ص 444.

الهدف منع الهجوم فحسب بل ضمان استمرارية الأعمال والقدرة على استعادة النظام لحيويته بعد التعرض للاختراق التقني.

محليا استشعر المشرع الجزائري خطورة التهديدات المحدقة بالمنظومات المعلوماتية للمؤسسات والأفراد وهو ما ترجمه من خلال صياغة إطار قانوني يعكس استيعابا دقيقا لمقتضيات البيئة الرقمية. فقد تضمن القانون رقم 18-04 المتعلق بالقواعد العامة للبريد والاتصالات الإلكترونية تعريفا صريحا ينص على أن الأمن السيبراني هو مجموع الأدوات والسياسات ومفاهيم الأمن والآليات الأمنية والمبادئ التوجيهية وطرق تسيير المخاطر التي يمكن استخدامها في حماية الاتصالات الإلكترونية ضد أي حدث من شأنه المساس بتوفر وسلامة وسرية البيانات المخزنة أو المعالجة أو المرسلة.[1]

يعكس هذا التدخل التشريعي وعيا حقيقيا بأن حماية بيانات العملاء داخل المؤسسات الخدمية لم تعد مجرد ممارسة تكنولوجية اختيارية بل أصبحت التزاما قانونيا يوجب على متخذي القرار اتخاذ كافة التدابير الوقائية لضمان الموثوقية الرقمية وعدم تعريض خصوصية الأفراد لانتهاكات الشبكات المفتوحة.

ثانياً: التمييز بين الأمن السيبراني وأمن المعلومات

يطفو على السطح الأكاديمي والمهني خلط شائع في استخدام مصطلحي الأمن السيبراني وأمن المعلومات كمرادفين يعبران عن ذات الغاية التنظيمية. غير أن التفكيك التحليلي الدقيق لطبيعة كلا الحقلين يكشف عن فوارق جوهرية وحساسة تتعلق بنطاق الحماية وطبيعة الأصول المحمية ونوعية التهديدات التي يتم التصدي لها، رغم وجود مساحة تقاطع حتمية بينهما تفرضها بيئة العمل الرقمية الحديثة التي تعتمدها المؤسسات التسويقية.

يعتبر أمن المعلومات المظلة الكبرى والأقدم تاريخيا حيث يرتكز جوهره على حماية المعلومة في حد ذاتها بغض النظر عن الوسيط الذي يحملها أو الشكل الذي تتخذه في الواقع. يهتم هذا الحقل بتوفير الحماية لكافة البيانات سواء كانت في شكل مستندات ورقية محفوظة في خزائن مادية، أو معلومات متداولة شفهيا بين الموظفين، أو بيانات مخزنة على أجهزة إلكترونية. الهدف المركزي لأمن المعلومات هو تطبيق الثالوث المعروف المتمثل في السرية والسلامة والتوافر، وذلك لمنع أي وصول غير مصرح به أو تعديل أو إتلاف للبيانات من قبل أي مصدر كان داخليا أو خارجيا وبغض النظر عن الوسيلة المستخدمة في هذا الاختراق.[2]

بالمقابل يتميز الأمن السيبراني بنطاق تشغيلي أضيق لكنه أشد تعقيدا وديناميكية من الناحية التكنولوجية. ينحصر اهتمام الأمن السيبراني حصريا في الفضاء الافتراضي والمجال الرقمي حيث يتمحور

[1] الجمهورية الجزائرية الديمقراطية الشعبية، قانون رقم 18-04، المتعلق بالقواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، الجريدة الرسمية، العدد 27، الجزائر، 2018، ص 7.

[2] وكال نور الدين، زقرير نصيرة، مدخل إلى الأمن المعلوماتي، الملتقى الدولي، جامعة البويرة، الجزائر، 2021، ص 39.

حول حماية البيانات الموجودة في شكل إلكتروني فقط وتأمين البنية التحتية التي تعالج وتخزن هذه البيانات مثل الخوادم والشبكات والأجهزة المحمولة والتطبيقات المفتوحة على الإنترنت. لا يلتفت الأمن السيبراني إلى الوثائق الورقية المادية المودعة في مكتب الإدارة أو الأرشيف الكلاسيكي، بل يركز جهده الدفاعي على التصدي للخطر القادم عبر الشبكات ومكافحة جرائم الاختراق والتصيد الاحتيالي والبرمجيات الخبيثة التي تستهدف خوادم المؤسسات. [1]

تبرز نقطة التباين الأكثر دلالة عند تحليل طبيعة التهديدات التي يتعامل معها كل مجال. بينما يتدخل خبير أمن المعلومات لحماية أرشيف المؤسسة من خطر الحريق أو الفيضان أو السرقة المادية المباشرة، يتدخل خبير الأمن السيبراني حين يحاول مقرصن مجهول الهوية يقبع في قارة أخرى اختراق قاعدة بيانات المؤسسة عن بعد واستخراج ملفات العملاء منها أو تشفيرها للمطالبة بفدية مالية. إن جرائم الإنترنت والقرصنة هي المجال الحصري للأمن السيبراني، بينما يغطي أمن المعلومات أي نشاط يهدد المعلومة ولو كان بسيطا كإفشاء سر مهني أثناء محادثة غير رسمية بين عاملين.

في سياق التسويق الخدماتي تبرز خطورة هذا التقاطع بشكل جلي. بيانات العملاء المتمثلة في مسارات التصفح والأرقام الائتمانية والمعرفات الشخصية هي أصول رقمية بحتة. وبالتالي فإن تأمين هذه البيانات يتطلب استراتيجية مزدوجة ترتكز على سياسات أمن معلومات تحدد من يحق له من الموظفين الاطلاع على هذه البيانات للحد من التهديد الداخلي، وأدوات أمن سيبراني متطورة تمنع القراصنة من اختراق الشبكة وسرقتها للحد من التهديد الخارجي.

ورغم هذه الفروق التنظيرية فإن تقاطع الحقلين يصبح حتميا واندماجيا في مؤسسات الخدمات المعاصرة. مع التحول الرقمي الشامل تلاشت تقريبا البيانات الورقية لصالح السجلات الإلكترونية وقواعد البيانات السحابية، مما يجعل الغالبية العظمى من أصول المعلومات داخل المؤسسات موجودة حصرا في الفضاء السيبراني. بناء على ذلك يصبح الأمن السيبراني هو الذراع التنفيذية الأهم والأقوى لأمن المعلومات. لا يمكن للمؤسسة أن تدعي تطبيق سياسة أمن معلومات صارمة لحماية سجلات زبائنها، إن لم تكن تمتلك في ذات الوقت بنية أمن سيبراني قادرة على صد الهجمات وتشفير قواعد البيانات وحماية مسارات التصفح الرقمية للعملاء من الاختراق والاستغلال غير المشروع الذي يدمر القيمة التسويقية للمنظمة.

المطلب الثاني: أهداف الأمن السيبراني في المؤسسات

تتجاوز المنظمات الخدمية المعاصرة في تعاطيها مع الفضاء الرقمي النظرة التقنية الضيقة للأمن السيبراني بوصفه مجرد برمجيات دفاعية لصد الاختراقات، لترتقي به إلى مصاف الركائز الاستراتيجية العليا التي تضمن بقاء الكيان المؤسسي واستدامته في بيئة شديدة العدائية. إن الغاية الجوهرية من إرساء

[1] نفس المرجع السابق، ص 40.

منظومة سيبرانية متكاملة داخل المؤسسات لا تقتصر على ردع الهجمات في لحظة وقوعها، بل تتسع لتشمل بناء ما يعرف بالمرونة السيبرانية، وهي القدرة الفائقة على استباق التهديدات، واحتواء الحوادث الرقمية المعقدة، والتعافي السريع لضمان استمرارية الأعمال بأقل تكلفة ممكنة، مع تحقيق توازن دقيق بين تمكين الابتكار في الخدمات الرقمية وضمان حماية الخصوصية المطلقة لبيانات العملاء. ويتفرع عن هذه الرؤية الاستراتيجية الكبرى نسق تحليلي مترابط من الأهداف التشغيلية والقانونية والتسويقية التي تعمل ككتلة واحدة لحماية أصول المنظمة ومكتسباتها.

يبرز هدف ضمان استمرارية الأعمال والجاهزية التشغيلية كأحد أهم المرتكزات التي تسعى المؤسسات لتحقيقها بصرامة تامة من خلال برامجها الأمنية. في بيئة التسويق الخدماتي التي تعتمد كليا على التدفق اللحظي للبيانات وتقديم الخدمات عبر البوابات الرقمية وتطبيقات الهواتف الذكية على مدار الساعة، يشكل أي انقطاع أو حجب للخدمة خسارة اقتصادية فادحة وضربة قاصمة للقيمة المدركة لدى المستهلك. يتدخل الأمن السيبراني هنا كآلية استباقية لمنع تعطيل العمليات التجارية، من خلال التصدي المباشر لهجمات حجب الخدمة الموزعة التي تهدف إلى إغراق خوادم المؤسسة بالبيانات الوهمية، وتوفير أنظمة النسخ الاحتياطي اللحظي، ووضع خطط دقيقة للتعافي من الكوارث. هذه الإجراءات تضمن بقاء الأنظمة وقواعد بيانات إدارة علاقات العملاء متاحة للمسوقين والمستهلكين عند الحاجة، وتقلص إلى أدنى حد ممكن فترات التوقف الناتجة عن الأعطال الفنية أو الهجمات الموجهة كبرمجيات الفدية التي تسعى لتشفير أصول الشركة وشل حركتها.

يحتل هدف حماية السرية والخصوصية المطلقة للبيانات صدارة الأولويات الأمنية غير القابلة للتفاوض. تمثل بيانات العملاء المادة الخام والمحرك الفعلي الذي تبنى عليه السياسات التسويقية الحديثة، بدءا من التفضيلات الاستهلاكية وصولا إلى المعلومات الائتمانية والبنكية. تسعى التدابير السيبرانية إلى فرض جدار عازل يمنع الوصول غير المصرح به إلى هذه المعلومات الشخصية، وذلك عبر توظيف بروتوكولات التشفير المعقدة للبيانات أثناء التخزين والنقل، وإدارة صلاحيات الدخول الصارمة التي تقيد ولوج الموظفين وفق مبدأ الحاجة إلى المعرفة. هذا المنع القاطع للتسريب أو التجسس يضمن بقاء الأصول المعلوماتية الحساسة بعيدة عن متناول القراصنة والشبكات الإجرامية المنظمة، ويحول دون تحول هذه البيانات إلى سلعة تباع في الأسواق السوداء للفضاء الافتراضي المظلم، مما يجسد الاحترام الفعلي والعملي للخصوصية الرقمية للمتعاملين مع المؤسسة.[1]

تتكامل حماية السرية كليا مع هدف محوري آخر يتمثل في تكريس سلامة البيانات ونزاهتها، وهو هدف يكتسي خطورة بالغة في السياق التسويقي والإداري المعاصر. التهديدات السيبرانية الراهنة لم تعد تقتصر على سرقة المعلومات فقط، بل تتعداها إلى محاولات التلاعب الخبيث بمحتواها وتغيير بنيتها

[1] منى الأشقر جبور، الأمن السايبري تحديات ومستلزمات المواجهة، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، 2017، ص 26.

المنطقية، كتعديل تفضيلات العملاء بغرض تضليل الخوارزميات التسويقية، أو تزوير سجلات الفوترة، أو تغيير شفرات البرامج التشغيلية لزرع أبواب خلفية. تعمل أدوات الأمن السيبراني المتقدمة على إحباط هذه المحاولات لضمان بقاء البيانات دقيقة، وأصيلة، وغير مشوهة، مطابقة تماما لحالتها الأصلية عند إدخالها من طرف العميل. يتعزز هذا الهدف بضمان صدق التصرفات الإلكترونية، عبر تتبع الأثر الرقمي لكل عملية وتوثيقها بآليات التوقيع الرقمي، مما يمنع ظاهرة الإنكار من قبل أي طرف، ويضفي حجية تقنية وقانونية قاطعة على التبادلات التعاقدية التي تجري عبر الشبكات المفتوحة، ليكون النظام المعلوماتي ذا موثوقية عالية تمنع أي تلاعب داخلي أو خارجي.[1]

يبرز الامتثال القانوني والتنظيمي كهدف إلزامي تسعى المؤسسات جاهدة لبلوغه لتجنب المساءلات والعقوبات المدمرة التي تفرضها بيئة الأعمال الحديثة. أفرزت التحولات الرقمية المتسارعة ترسانة من القوانين المحلية والدولية الصارمة المتعلقة بحماية البيانات الشخصية، كنظام حماية البيانات الشخصية السعودي أو اللائحة العامة لحماية البيانات في أوروبا، أو القوانين الجزائرية المتعلقة بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات. إرساء منظومة أمن سيبراني قوية ومتوافقة مع المعايير الدولية كمعيار الآيزو يسمح للمؤسسة بالتوافق التام مع هذه المتطلبات التشريعية، وتفادي الغرامات المالية الضخمة والتبعات القضائية التي تفرض على الجهات التي تثبت إدانتها بالتقصير في حماية بيانات عملائها. يعد تحقيق هذا الامتثال دليلا ملموسا على ارتقاء المنظمة إلى مستويات النضج المؤسسي، حيث يتحول الأمن من مجرد التزام تقني يقع على عاتق مهندسي الشبكات، إلى ممارسة حوكمية استراتيجية وشفافة تثبت من خلالها الإدارة العليا مسؤوليتها المطلقة تجاه أصولها ومحيطها الخارجي وتدعم توجهات الدولة في فرض سيادتها الرقمية على البيانات المتداولة داخل حدودها.

ينصهر هذا النسق المعقد من الأهداف الوقائية والتنظيمية والقانونية ليصب في النهاية في بوتقة الهدف التسويقي الأسمى، والمتمثل في بناء الثقة الرقمية وخلق الميزة التنافسية المستدامة. في أسواق إلكترونية تتسم بتجانس الخدمات واشتداد المنافسة وسرعة انتقال العميل بين مقدمي الخدمة بنقرة زر، لم يعد المستهلك الرقمي يقيم الخدمة بناء على جودتها الوظيفية أو سعرها فحسب، بل يضع معيار الموثوقية والأمان في صدارة محددات قرار الشراء والتفاعل. نجاح المؤسسة الخدمية في حماية كيانها الرقمي، ومنع تسرب بيانات بطاقات الائتمان، وإثبات مناعتها ضد الابتزاز الإلكتروني، يرسل إشارات طمأنة سيكولوجية عميقة للعملاء والشركاء تقضي على ظاهرة القلق الرقمي المرتبطة باستهلاك الخدمات اللاملموسة. تتحول هذه الثقة المتولدة تدريجيا إلى أصل تجاري استراتيجي غير ملموس، يعزز الولاء المؤسسي، ويرفع من قيمة العلامة التجارية، ويمنح المنظمة قدرة هجومية في السوق لجذب شرائح جديدة من العملاء الذين يبحثون عن الملاذات الرقمية الآمنة، مما يغير النظرة الكلاسيكية لميزانية الأمن

[1] منى الأشقر جبور، مرجع سبق ذكره، ص 26.

السيبراني من خانة التكاليف التشغيلية المرهقة، لتصبح استثمارا استراتيجيا يدر العوائد ويوسع الحصة السوقية.

يتطلب التجسيد الفعلي والميداني لهذه الأهداف التقنية والتسويقية تحقيق هدف بنيوي أخير يركز بشكل مكثف على هندسة الوعي السيبراني وتأهيل المورد البشري. تدرك مجالس إدارات المؤسسات الحديثة أن أعتى جدران الحماية البرمجية تنهار بسهولة تامة أمام خطأ بشري بسيط، أو هفوة من موظف يفتقر إلى الوعي الأمني ويقع ضحية لرسالة تصيد إلكتروني. يهدف البرنامج الأمني المتكامل إلى خلق ثقافة سيبرانية شاملة داخل أروقة المنظمة، تنتقل بالموظف من كونه الحلقة الأضعف والثغرة المحتملة التي يستغلها القراصنة، ليكون خط الدفاع الأول والدرع البشري الواقي للبيانات. يتحقق هذا الهدف العميق عبر التدريب المستمر على رصد محاولات التصيد الاحتيالي، وفهم آليات الهندسة الاجتماعية المعقدة التي تتالعب بالنفسيات، والالتزام الصارم ببروتوكولات إدارة كلمات المرور وتشفير الملفات الحساسة، مما يضمن تسييج المحيط الرقمي للمؤسسة بوعي إنساني متيقظ يكمل دور الخوارزميات الدفاعية ويسد ثغراتها المتبقية.[1]

المطلب الثالث: مبادئ الأمن السيبراني المرتبطة بحماية البيانات

تستند البنية المعمارية لأي استراتيجية دفاعية في الفضاء الرقمي إلى نسق من المبادئ التوجيهية الصارمة التي تحدد مسارات العمل وتحكم السياسات التقنية والإدارية داخل المنظمة الخدمية. لم يأت تصميم هذه المبادئ كاستجابة عشوائية للتهديدات المتطورة، بل تبلور عبر عقود من تراكم المعرفة التقنية وتطور الممارسات الإدارية ليفرز نموذجا معياريا يمثل النواة الصلبة للأمن السيبراني وأمن المعلومات على حد سواء. يعرف هذا النموذج أكاديميا ومهنيا بمثلث الحماية، والذي يشكل حجر الزاوية الذي تبنى عليه كافة بروتوكولات تأمين الشبكات وقواعد البيانات، ويعتبر المعيار المرجعي الأساسي لتقييم كفاءة وموثوقية النظم المعلوماتية وتحديد قدرتها على الصمود أمام محاولات الاختراق الخبيثة.

يقوم هذا النموذج المفاهيمي على فكرة مركزية عميقة مفادها أن المعلومات تكتسب قيمتها الاقتصادية والتسويقية الحقيقية من خلال توافر ثلاث خصائص حيوية متلازمة لا تقبل التجزئة. إن أي خلل هيكلي يصيب إحدى هذه الركائز يؤدي بالضرورة الحتمية إلى انهيار المنظومة الأمنية بأكملها، مما يحول البيانات من أصل استراتيجي منتج للقيمة وموجه للقرار، إلى عبء قانوني ومصدر للتهديد الوجودي الذي يعصف بكيان المؤسسة.[2]

في سياق التسويق الخدماتي المعاصر، تكتسي هذه المبادئ أهمية استثنائية تتجاوز البعد التكنولوجي البحت. لم تعد هذه المعايير حكرا على مهندسي الشبكات ومسؤولي الأنظمة، بل تحولت إلى

[1] أويس مجيد غالب العوادي، مرجع سبق ذكره، ص 4.

[2] وكال نور الدين، زقرير نصيرة، مرجع سبق ذكره، ص 39.

التزامات تعاقدية وضمانات أخلاقية تربط المنظمة بعملائها في الفضاء الافتراضي. فالعميل الرقمي الذي يتفاعل مع المنصات الخدمية ويدلي بمعطياته الشخصية والسلوكية والمصرفية، يضع ثقته الكاملة في قدرة المؤسسة على تطبيق هذه المبادئ بصرامة تامة تضمن عدم انكشاف هويته.

وبناء على هذا التداخل العضوي الحرج بين التقنية المتطورة وإدارة علاقات الزبائن، يستوجب التحليل المنهجي تفكيك هذه المبادئ المركزية تباعا، ودراسة آليات ارتباطها المباشر والعملي بحماية بيانات العملاء. يفرض هذا المسار التحليلي الانطلاق من فحص الركيزة الأولى والأكثر حساسية في بناء الثقة، والمتمثلة في مبدأ السرية والموثوقية، لفهم كيف تتضافر التكنولوجيا مع السياسات الإدارية لخلق جدار عازل يحمي المستهلك من الانكشاف.

أولا: مبدأ السرية والموثوقية (Confidentiality)

يحتل مبدأ السرية موقع الصدارة ضمن هرم الأولويات الأمنية للمنظمات، ويمثل خط الدفاع الأول والأساسي الذي يحول دون انكشاف الأصول الرقمية للكيانات غير المصرح لها بالوصول. يقصد بالسرية في القاموس السيبراني والتشريعي ذلك النسق المعقد من القيود الصارمة والإجراءات المعتمدة التي تضمن بقاء المعلومات محجوبة تماما عن أي أفراد، أو أنظمة، أو عمليات برمجية لا تملك تفويضا رسميا للولوج إليها. يتضمن هذا المفهوم بشكل جوهري توفير كافة الوسائل التقنية والتنظيمية لحماية الخصوصية الفردية للعملاء والحفاظ على ملكية المعلومات التجارية، حيث يعتبر أي إفشاء أو تسريب لهذه المعطيات، سواء تم بقصد اختراقي من قبل قراصنة أو بخطأ تشغيلي غير مقصود من قبل الموظفين، انهيارا كاملا لمبدأ السرية.[1]

يعمل هذا المبدأ كحاجز رقمي غير مرئي ومستمر. وتتطلب ترجمة هذا المبدأ النظري إلى واقع تشغيلي فعال بناء معمارية دفاعية متعددة الطبقات والمستويات. تبدأ هذه المعمارية بتفعيل سياسات التحكم في الوصول، وهي آليات تقنية صارمة تفرض على المنظمة عدم إتاحة البيانات للجميع، بل يتم تقييد الصلاحيات استنادا إلى قاعدة الحاجة إلى المعرفة. يعني هذا الإجراء الإداري أن موظف قسم التسويق يمنح فقط القدرة المحدودة على رؤية البيانات الديموغرافية الضرورية لتوجيه حملة إعلانية مخصصة، في حين يحرم من الناحية البرمجية من الوصول إلى السجلات الائتمانية أو كلمات المرور الحساسة الخاصة بالعميل. تعتمد أنظمة التحكم في الوصول على إجراءات توثيق هوية قوية، تتجاوز الاعتماد الكلاسيكي والضعيف على كلمات المرور البسيطة لتشمل تقنيات المصادقة الثنائية والمصادقة البيومترية التي تحلل الخصائص الفسيولوجية للمستخدم لضمان استحالة انتحال الشخصية.[2]

[1] المعهد الوطني للمعايير والتكنولوجيا NIST، مقدمة في أمن المعلومات SP 800-12r1، دون طبعة، وزارة التجارة الأمريكية، الولايات المتحدة الأمريكية، 2017، ص 3.

[2] كودي أ. كوكران، مرجع سبق ذكره، ص 18.

يمتد تطبيق السرية ليعتمد بشكل جذري وحتمي على تكنولوجيا التشفير العكسي، والتي تمثل حجر الزاوية الفعلي في حماية البيانات البالغة الحساسية. يقوم التشفير بتحويل المعطيات الواضحة والمقروءة إلى سلسلة من الرموز المعقدة والطلاسم الرياضية التي يستحيل فكها أو فهم محتواها دون امتلاك مفتاح التشفير السري الخاص بها. تلعب هذه التقنية الاستراتيجية دورا مزدوجا في حماية البيانات أثناء وجودها في حالة سكون داخل خوادم التخزين، وتحميها كذلك وهي في حالة حركة وانتقال عبر شبكات الاتصال المفتوحة. فحتى لو تمكن مقرصن محترف من تجاوز الجدران النارية والسطو على قاعدة البيانات، فإن مبدأ السرية يبقى مصانا بفضل التشفير الذي يحول تلك الغنيمة الرقمية إلى كتل بيانات مشوهة وعديمة المنفعة.[1]

من الناحية التحليلية والقانونية، يبرز تداخل مفاهيمي حاد في الأدبيات بين مصطلحي السرية والخصوصية، رغم وجود فوارق هيكلية قاطعة بينهما تحدد طبيعة المسؤولية المؤسسية. ترتبط الخصوصية بالحق السيادي للعميل في السيطرة الكاملة على بياناته، وتحديد نطاق ما يمكن جمعه منها والموافقة المسبقة على من يحق له معالجتها أو مشاركتها. في المقابل، تعتبر السرية الأداة التقنية والتشغيلية المباشرة التي تطبقها المنظمة للوفاء بوعد الخصوصية وتجسيده على أرض الواقع. الخصوصية هي الغاية التشريعية، بينما السرية هي الآلية السيبرانية التي تضمن عدم الإفراج عن تلك المعطيات الشخصية إلا وفقا للقيود المتفق عليها، مما يجعل الأمن السيبراني الداعم الأول والمنفذ الفعلي للخصوصية.[2]

ينعكس هذا التطبيق الصارم لمعايير السرية بشكل مباشر وقوي على المردودية التسويقية للمؤسسات الخدمية. في أسواق رقمية تتميز بحدة المنافسة المفرطة وتطابق البدائل، يتحول الالتزام التام بسرعة وأمان المعاملات إلى ميزة تنافسية حاسمة ترجح كفة مؤسسة على أخرى. إن إدراك المستهلك بأن المنظمة تتبنى بروتوكولات حماية متطورة تمنع أي وصول خارجي لبياناته المالية ومسارات تصفحه، يؤدي إلى تخفيض جذري في مستويات القلق الرقمي المرتبط باستهلاك الخدمات اللاملموسة. هذا الانخفاض في الإدراك بالتهديدات هو المولد الفعلي لتعزيز الثقة الإلكترونية، والذي يترجم إلى ولاء مؤسسي واستعداد مطلق للانخراط في علاقات تجارية ممتدة.

على النقيض تماما، يؤدي أي تفريط منهجي أو تقني في مبدأ السرية إلى تداعيات تدميرية تتجاوز الخسارة المالية المؤقتة لتضرب صميم العقد النفسي مع الزبون. إن حوادث كشف البيانات الشخصية وتسريبها للعلن، والتي تزايدت وتيرتها بشراسة مع تطور هجمات التصيد الاحتيالي وبرمجيات الفدية، تدمر السمعة المؤسسية وتنسف الصورة الذهنية للعلامة التجارية في لحظات. تدفع هذه الحوادث الخطيرة

[1] ذيب بن عايض القحطاني، أمن المعلومات، دون طبعة، دار قابس للطباعة والنشر والتوزيع، لبنان، 2015، ص 91.

[2] فرانس بيلانجر، روبرت كروسلر، أبحاث خصوصية المعلومات: مراجعة متعددة التخصصات، مجلة ربع سنوية لنظم المعلومات، العدد 4، المجلد 35، جامعة فرجينيا للتكنولوجيا، الولايات المتحدة الأمريكية، 2011، ص 1020.

العملاء المتضررين إلى تبني مقاطعة فورية للخدمات الإلكترونية للمنظمة المخترقة والانتقال الجماعي نحو منافسين يوفرون بيئة أكثر رصانة. يؤكد هذا الواقع التشغيلي أن الحفاظ على سرية البيانات لم يعد خيارا ترفيهيا قابلا للتأجيل، بل هو شريان الحياة الذي يضمن بقاء المؤسسات وقدرتها على تحقيق أهدافها الربحية والاستراتيجية.[1]

تستدعي الإدارة الشاملة لمبدأ السرية إرساء ثقافة تنظيمية تتجاوز الحلول البرمجية الجاهزة، لتركز على العامل البشري باعتباره الحلقة الأضعف في سلسلة التأمين. إن الاستثمار الضخم في خوارزميات التشفير يفقد فعاليته كليا إذا قام موظف غير مدرب بالاحتفاظ بكلمة المرور الخاصة به في مكان مكشوف، أو استجاب لرسالة هندسة اجتماعية خادعة قادته لتسليم مفاتيح الولوج للشبكة عن طواعية للمخترقين. يفرض هذا التحدي على الإدارة العليا تصميم برامج توعية مستمرة تدمج الموظفين ضمن هيكل الحماية، وتحولهم من مصادر للتهديد الداخلي المحتمل إلى جدار حماية بشري يدرك تماما حساسية البيانات التي يتعامل معها، ويعي العواقب الوخيمة المترتبة عن أي تساهل في تطبيق بروتوكولات السرية المعتمدة.[2]

ثانيا: مبدأ السلامة والنزاهة (Integrity)

يتجاوز الفهم المعاصر لحماية الأصول الرقمية مجرد إخفاء البيانات عن الأعين المتلصصة، ليمتد نحو ضمان موثوقية هذه المعطيات وعدم تعرضها للتشويه الخفي. يبرز مبدأ السلامة والنزاهة كركيزة دفاعية تضمن بقاء المعلومات على حالتها الأصلية الدقيقة، ويقصد به توفير الحماية المطلقة للبيانات من أي تعديل، إضافة، حذف، أو تدمير غير مصرح به، سواء تم ذلك بصفة متعمدة عبر هجمات الاختراق، أو بصفة عرضية نتيجة أخطاء تشغيلية داخلية. تشمل السلامة في الأدبيات الأمنية شقين متكاملين لا ينفصلان؛ يتعلق الأول بسلامة البيانات ذاتها وحفظ محتواها أثناء التخزين والمعالجة والانتقال عبر الشبكات المفتوحة، في حين ينصرف الشق الثاني إلى سلامة النظام المبرمج ككل، مما يضمن أداءه لوظائفه التشغيلية دون أي تلاعب داخلي أو خارجي يمس بمنطق المعالجة.[3]

تكتسي هذه الركيزة الأمنية طابعا حساسا ومفصليا في بيئة التسويق الخدماتي التي تبني قراراتها حصريا على قواعد البيانات. إن اختراقا يمس نزاهة البيانات، كتعديل خبيث في التفضيلات الشرائية لعميل معين، أو تلاعب في سجلات الفوترة الإلكترونية، أو تغيير مسارات التسليم، لا يقل خطورة وفتكا من تسريب تلك البيانات للعلن. يؤدي هذا التشويه المعلوماتي إلى توجيه رسائل تسويقية خاطئة وتقديم

[1] طارق إبراهيم الدسوقي عطية، مرجع سبق ذكره، ص 38.

[2] محمد عبد الله شاهين، الأمن السيبراني ونظم حماية المعلومات، الطبعة الأولى، دار يافا العلمية للنشر والتوزيع، الأردن، 2023، ص 8.

[3] وكال نور الدين، زقرير نصيرة، مدخل إلى الأمن المعلوماتي، الملتقى الدولي، جامعة البويرة، 2021، ص 39.

خدمات لا تتطابق مع توقعات الزبون، وهو ما يعصف فورا بالقيمة المدركة للخدمة ويدمر الثقة المؤسسية بشكل يصعب ترميمه.

لتحقيق هذا المبدأ من الناحية التقنية، تعتمد بروتوكولات الأمن السيبراني المتقدمة على آليات مجهرية صارمة. يتمثل أبرزها في استخدام خوارزميات دالة التجزئة الرياضية التي تقوم بتوليد بصمة رقمية فريدة لكل كتلة بيانية، مما يسمح باكتشاف أي تغيير ولو كان بحجم بت واحد يطرأ على الملف أثناء نقله. تضاف إلى ذلك تقنيات التوقيع الرقمي التي تضمن صدق التصرفات الإلكترونية وعدم إنكارها من قبل الأطراف المتعاقدة، وتطبيق سياسات إدارة الصلاحيات التي تمنع الموظفين غير المخولين من إجراء أي تعديلات على سجلات العملاء الحساسة، مقيدة إياهم بصلاحية القراءة فقط متى استدعت الحاجة التشغيلية ذلك.[1]

يفرض الواقع التجاري للمؤسسات الخدمية وضع مبدأ النزاهة في صدارة الأولويات الهيكلية، وهو ما تؤكده النماذج الأمنية المتقدمة التي تم تصميمها خصيصا للبيئات التجارية، حيث تعتبر أن الحفاظ على الاتساق الداخلي للبيانات وتطابقها التام مع الواقع الخارجي يمثل شريان الحياة للعمليات التعاقدية الرقمية. إن فقدان النزاهة يعني أن متخذ القرار التسويقي يبني استراتيجياته التوسعية واستثماراته المالية على أسس وهمية وبيانات مضللة، مما يقود المؤسسة نحو قرارات كارثية تعزلها عن سوقها الحقيقي وتفقدها بوصلة التوجيه السلوكي للمستهلكين.

تتضح لنا قوة هذا المبدأ حين يتم ربطه بعمليات التدقيق المستمرة التي تفرضها القوانين الحديثة. فالمؤسسة ملزمة قانونا بضمان أن السجلات المجمعة عن المواطنين تعكس الحقيقة دون تحريف، وأن أي نظام يعالج هذه المعطيات يمتلك مناعة ذاتية ترفض حقن الأكواد الخبيثة أو البرمجيات التي تسعى لتغيير مخرجات الخوادم، مما يجعل النزاهة رديفا للشفافية المطلقة.

ثالثا: مبدأ التوافر وإمكانية الوصول (Availability)

لا تحمل كتل البيانات البالغة السرية والدقيقة أي قيمة اقتصادية أو تسويقية فعلية إن كانت محجوبة عن متخذي القرار أو عن العملاء في اللحظة الحرجة التي يطلبونها فيها. يتبلور مبدأ التوافر كعنصر تشغيلي يحكم الجاهزية الدائمة والحيوية للنظم المعلوماتية، ويعرف بأنه الضمان التقني والإداري الذي يكفل للمستخدمين المصرح لهم الوصول إلى البيانات والموارد الشبكية واستخدامها في الوقت المناسب وبشكل موثوق، دون أي عوائق أو انقطاعات زمنية تتجاوز الحدود المسموح بها. يتطلب هذا المبدأ هندسة البنية التحتية بطريقة استباقية تضمن استمرارية الأعمال تحت أسوأ الظروف، وهو ما يفرض توفير أجهزة الخوادم ببدائل طاقة احتياطية، والاعتماد المطلق على أنظمة النسخ الاحتياطي

[1] ذيب بن عايض القحطاني، أمن المعلومات، دار قابس للطباعة والنشر والتوزيع، لبنان، 2015، ص 91.

اللحظي ونقل البيانات إلى محركات أقراص خارجية أو سحابات مؤمنة، وتصميم مسارات شبكية متكررة تمنع تعطل الخدمة إذا فشل أحد المكونات المركزية.[1]

يواجه هذا المبدأ تهديدات سيبرانية شرسة تأخذ طابعا تخريبيا وابتزازيا، وعلى رأسها هجمات حجب الخدمة الموزعة التي تعمد إلى إغراق خوادم المنظمة الخدمية بملايين الطلبات الوهمية في أجزاء من الثانية، مما يؤدي إلى شلل تام في قدرة النظام على معالجة طلبات العملاء الحقيقيين. يضاف إلى ذلك الخطر المتنامي لبرمجيات الفدية الخبيثة التي تقوم بتشفير قواعد بيانات المؤسسة بالكامل، وتحجبها عن الموظفين والعملاء لحين دفع مبالغ مالية ضخمة. في قطاع الخدمات تحديدا، والذي يتسم بالتلازم الحتمي بين لحظة التقديم ولحظة الاستهلاك، يؤدي عدم التوافر إلى شل النشاط الاقتصادي وتكبيد المنظمة خسائر مالية فورية لا يمكن تعويضها، فمبيعات الخدمة الضائعة اليوم لا يمكن تخزينها لبيعها غدا.

العميل الرقمي المعاصر الذي يعجز عن الولوج إلى حسابه البنكي الإلكتروني لتسديد التزاماته، أو يواجه رفضا تقنيا في إتمام عملية دفع رقمية بسبب تعطل النظام المركزي للمنظمة، يتولد لديه إدراك سيكولوجي مباشر بهشاشة هذه المؤسسة وتخلف بنيتها التكنولوجية. يترجم هذا الإدراك السلبي فورا إلى تآكل حاد في معدلات الولاء، ويدفع المستهلك نحو البحث المباشر عن بدائل تنافسية توفر بيئة استهلاك مستقرة وخالية من الاحتكاك المزعج. بناء على ذلك، يتحول الأمن السيبراني عبر تأمينه الصارم لمبدأ التوافر من مجرد درع حماية تقني يقبع في الغرف الخلفية للإدارة، إلى أداة تسويقية هجومية تروج لجودة الخدمة وموثوقيتها، وتجذب شرائح عملاء تبحث عن الاستقرار الرقمي.[2]

يرتبط ضمان التوافر ارتباطا عضويا بالقدرة المؤسسية على إدارة الأزمات والتعافي السريع من الكوارث الرقمية وتجاوز نقطة الإخفاق بأقل تكلفة زمنية ممكنة. إن تصميم خطط الاستجابة الفورية، واسترجاع السجلات المعطوبة من النسخ الاحتياطية الموزعة جغرافيا، يعكس النضج الاستراتيجي للمؤسسة، ويثبت للمساهمين والعملاء أن المنظمة تمتلك مرونة سيبرانية تمكنها من امتصاص الصدمات والعودة إلى نشاطها الطبيعي بفاعلية تامة، محولة بذلك التهديد الخارجي إلى فرصة لاستعراض كفاءتها التقنية وصلابتها التنظيمية في السوق.

[1] ابتسام أونيس، حوفاء مطروح، تداعيات جائحة كوفيد-19 وتأثيرها على تحقيق الأمن السيبراني في الجزائر، مجلة دراسات وأبحاث، دون عدد، دون هيئة مصدرة، 2021، ص 4.

[2] سيد ماهر بدوي عبد الله، أثر ثقة العميل في المؤسسة المصرفية على قبوله التعامل المصرفي عبر الإنترنت، رسالة ماجستير، إدارة الأعمال، كلية التجارة، جامعة القاهرة، مصر، 2013، ص 58.

المبحث الثاني: فعالية الأمن السيبراني في حماية بيانات العملاء

يستوجب الانتقال من التنظير الاستراتيجي إلى الممارسة الميدانية في حقل حماية الأصول الرقمية، بناء فهم تشغيلي دقيق لكيفية تفاعل الأنظمة الدفاعية مع التهديدات المتصاعدة في بيئة الأعمال المعاصرة. لا تكتفي المؤسسة الخدمية بإدراك الأهمية الاقتصادية لبيانات عملائها أو وضع أهداف نظرية لحمايتها، بل يتطلب الأمر ترجمة هذه الأهداف إلى واقع ملموس عبر تفعيل آليات دفاعية قادرة على الصمود وامتصاص الصدمات السيبرانية. يعالج هذا المبحث الجانب التطبيقي للأمن السيبراني، مستعرضا الآليات التقنية والتنظيمية المعتمدة لصد الاختراقات، لينتقل إلى تحليل الانعكاسات المباشرة لهذه الفعالية على السلوك الاستهلاكي، وتحديدا في قدرتها على تكريس الموثوقية الرقمية وخلق الميزة التنافسية التي تضمن استدامة العلاقة التسويقية.

المطلب الأول: آليات الأمن السيبراني لحماية بيانات العملاء

لا تختزل منظومة الحماية السيبرانية في مجرد اقتناء برمجيات معقدة أو تنصيب خوادم متطورة، بل هي هندسة متكاملة تتطلب تضافر جهود الآلة والعنصر البشري في نسق واحد. يرتكز بناء هذا الجدار الرقمي على مسارين متوازيين؛ مسار تقني يتولى معالجة البيانات وتشفيرها ومراقبة حركتها، ومسار تنظيمي إداري يتولى تأطير السلوك البشري وتحديد صلاحيات الوصول. يخلق هذا التلاحم العضوي بيئة محصنة قادرة على احتواء المخاطر التي تستهدف البصمة الرقمية للعميل.

أ. الآليات التقنية (التشفير، جدران الحماية، اكتشاف الاختراقات).

تمثل الآليات التقنية القاعدة الصلبة وخط الدفاع البرمجي الأول الذي تتصادم معه بصورة مباشرة أي محاولة اختراق تستهدف استنزاف قواعد بيانات المؤسسة. تتجسد هذه الآليات في حزمة من الحلول الخوارزمية والهندسية التي تعمل بصفة متزامنة ومستمرة لتنقية حركة مرور البيانات، ومنع تسرب السجلات الحساسة للعملاء نحو الفضاءات غير الآمنة أو الشبكات المظلمة. تأخذ هذه الحلول طابعا وقائيا وآخر علاجيا يهدف إلى تقليص مساحة الهجوم المتاحة أمام القراصنة.

تأتي تقنية التشفير في طليعة هذه التدابير الحيوية وأكثرها تعقيدا من الناحية الرياضية. وتعرف هذه التقنية بأنها العملية التي يتم من خلالها تحويل المعلومات والبيانات المقروءة إلى إشارات ورموز غير مفهومة وطلاسم معقدة باستخدام برنامج خاص، بحيث لا يمكن قراءتها أو إعادة بنائها منطقيا إلا بامتلاك المفتاح السري المخصص لذلك.[1]

تلعب خوارزميات التشفير دورا استراتيجيا مزدوجا يتمثل في تأمين البيانات خلال فترات تخزينها الساكنة على الخوادم المركزية الخاصة بالمنظمة، وحمايتها بقوة أثناء حركتها وانتقالها عبر قنوات

[1] طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، 2009، ص 38.

الاتصال المفتوحة. وحتى في أسوأ السيناريوهات الأمنية التي يتمكن فيها المهاجم الخارجي من تجاوز الجدران الحدودية والاستيلاء الفعلي على ملفات العملاء، تظل هذه الملفات مجرد كتل بيانية مشوهة وعديمة الجدوى. لا يمكن للمقرصن استخلاص أي نمط ديموغرافي أو ائتماني أو سلوكي منها لغياب مفتاح فك التشفير، وهو ما يجسد التطبيق العملي والصارم لمبدأ السرية المطلقة.[1]

بموازاة التشفير العكسي، تعتمد معمارية الشبكات الآمنة بشكل مكثف على جدران الحماية والتي تعتبر بمثابة نقاط التفتيش الافتراضية العازلة. تعمل هذه الجدران كحاجز تقني يفصل بين الشبكة المحلية الداخلية للمؤسسة والتي تحتوي على السجلات الخاصة، وبين شبكة الإنترنت الخارجية المليئة بالتهديدات والمخاطر. يرتكز عمل جدار النار كجهاز مادي أو برنامج مخصص على مراقبة وتصفية جميع البيانات الصادرة والواردة استنادا إلى مجموعة من القواعد الأمنية الصارمة المحددة سلفا من طرف الإدارة والمهندسين.[2]

تقوم هذه البوابات الإلكترونية بصد محاولات الوصول غير المصرح بها آليا، وتطلق إنذارات فورية في حال رصد تعليمات برمجية مشبوهة أو أوامر غير مسموح بها تحاول النفاذ إلى خوادم تخزين بيانات الزبائن. يتطلب إعداد وتكوين جدران حماية تتناسب مع حجم التدفق الهائل للبيانات التسويقية دقة متناهية، لضمان عدم التأثير على سرعة تقديم الخدمة للعميل الشرعي، وفي الوقت نفسه منع البرمجيات الخبيثة من الاستقرار داخل بيئة العمل.

تتجه المنظمات الخدمية الحديثة نحو تبني قدرات استباقية متقدمة من خلال نشر أنظمة اكتشاف الاختراقات ومنع التطفل.

توفر أنظمة الاكتشاف مسحا حيويا ومستمرا لكامل حركة مرور الشبكة، معتمدة على قواعد بيانات ضخمة تحتوي على البصمات المميزة للأساليب الهجومية المعروفة. تتعقب هذه البرمجيات الأنشطة غير الطبيعية والانحرافات السلوكية في مسارات التصفح وحركة البيانات، لتنبه المسؤولين بشكل فوري عند اكتشاف أي محاولة تسلل متخفية تتجاوز جدار الحماية.[3]

يمنح هذا الإنذار المبكر متخذ القرار القدرة الميدانية على التدخل في اللحظة الحرجة لغلق الثغرات وتجميد العمليات، وعزل الأجهزة المصابة عن باقي الشبكة، لمنع المهاجم من سحب السجلات أو تشويهها. يشكل هذا التلاحم العضوي بين التشفير، وجدران الحماية، وأنظمة الاكتشاف، بيئة تقنية صلبة يصعب اختراقها بالطرق التقليدية.

ب. الآليات التنظيمية والإدارية (سياسات الأمان، تدريب الموظفين).

[1] المرجع السابق، ص 40.

[2] ذيب بن عايض القحطاني، أمن المعلومات، الطبعة الأولى، دار قابس للطباعة والنشر والتوزيع، لبنان، 2015، ص 91.

[3] وكال نور الدين، زقرير نصيرة، مدخل إلى الأمن المعلوماتي، الملتقى الدولي، جامعة البويرة، الجزائر، 2021، ص 40.

تفقد الآليات التقنية مهما بلغت من تطور خوارزمي وصرامة برمجية فعاليتها الحقيقية إن لم تسند بهيكل تنظيمي متين يضبط حركة الموارد البشرية ويوجه تصرفاتها اليومية. يمثل العنصر البشري داخل المؤسسة الخدمية الحلقة الأضعف والمنفذ الأكثر استهدافا من قبل الفواعل الإجرامية نظرا لقابليته للتلاعب النفسي والإهمال. يجعل هذا الواقع التشغيلي التركيز على الجانب الإداري أمرا يوازي في خطورته وتأثيره شراء الخوادم المتطورة.

تبرز سياسات الأمان كوثيقة دستورية داخلية ترسم الحدود وتحدد المسؤوليات التشغيلية بدقة. تتمثل هذه السياسات في وضع أسس تنظيمية دقيقة وتطبيق لوائح صارمة للحفاظ على البيانات الخاصة بالشركة والموجودة على الأجهزة، وتوزيع المسؤوليات على الأفراد العاملين لضمان عدم وقوع المعلومات الحساسة للعملاء تحت سيطرة فرد واحد حصريا.[1]

تتفرع السياسات الأمنية لتشمل بروتوكولات حازمة تتعلق بآلية إنشاء وإدارة كلمات المرور وتحديثها الدوري، وفرض قيود صارمة على استخدام وسائط التخزين الخارجية التي تعد ناقلة صامتة للبرمجيات الخبيثة. وتلزم هذه اللوائح التنظيمية موظفي أقسام التسويق والمبيعات بالامتثال التام لمبدأ الحد الأدنى من الامتيازات. يرتكز هذا المبدأ الإداري على عدم منح الموظف صلاحية الاطلاع على السجلات الائتمانية أو الديموغرافية إلا بالقدر الذي يتطلبه أداء مهامه الوظيفية المباشرة.[2]

يقلص هذا التوجه بصورة درامية من احتمالات تسريب المعطيات بدافع الخطأ العرضي، أو التواطؤ العمدي مع جهات منافسة تبحث عن استغلال قواعد البيانات.

لإضفاء الصبغة القانونية والردعية، تلجأ المنظمات إلى توثيق الالتزام البشري عبر إبرام عقود واتفاقيات إلزامية. يكرس هذا الإجراء الطابع الرسمي للسرية، ويجعل الموظف يدرك العواقب المهنية والقضائية الوخيمة المترتبة عن إفشاء أسرار الزبائن أو بيع بياناتهم. غير أن الردع وحده يظل قاصرا عن بناء مرونة سيبرانية حقيقية.

يفرض نجاح هذه السياسات وتطبيقها الميداني إرفاقها ببرامج مكثفة لتدريب الموظفين وبناء الثقافة الرقمية المانعة. لا تستطيع سياسة مكتوبة أن تصد هجوما يعتمد على تقنيات الهندسة الاجتماعية إن كان الموظف يفتقر إلى الوعي الكافي لرصد الحيل الخبيثة. يرفع التدريب المنتظم للمورد البشري على مفاهيم الأمن السيبراني من مستوى يقظة العاملين، ويقلل من احتمالية الوقوع في فخاخ التصيد الاحتيالي التي ترد عبر رسائل البريد الإلكتروني وتستهدف سرقة بيانات الدخول.[3]

[1] محمد عبد الله شاهين، الأمن السيبراني ونظم حماية المعلومات، الطبعة الأولى، دار يافا العلمية للنشر والتوزيع، الأردن، 2023، ص 8.

[2] المرجع السابق، ص 10.

[3] أويس مجيد غالب العوادي، الأمن السيبراني المعلوماتي، سلسلة إصدار مركز الدراسات والتخطيط، العراق، 2016، ص 12.

يشمل التكوين التفاعلي إكساب الموظفين المهارات التقنية لتحديد الروابط المشبوهة، وفهم المخاطر القانونية الكارثية للانتهاكات. عندما تدمج الإدارة سياسات الردع والمراقبة مع التكوين المعرفي، فإنها تحول قواها العاملة من ثغرة داخلية تستنزف أمنها، إلى خط دفاع بشري متقدم يعزز مناعتها السيبرانية.

يستنتج بوضوح أن حماية بيانات العملاء لا تتأتى من الاعتماد على مسار أحادي. تعجز خوارزميات التشفير عن حماية نظام قرر مديره تسليم أرقامه السرية بحسن نية، ويقف الموظف المدرب عاجزا أمام هجمات حجب الخدمة إن لم توفر له الإدارة جدران حماية متطورة. إن التوافق الهيكلي بين الترسانة التقنية والبروتوكولات الإدارية هو المنتج الفعلي لبيئة رقمية موثوقة.

المطلب الثاني: دور الأمن السيبراني في تعزيز ثقة العملاء

تنتفي القيمة التشغيلية للآليات التقنية والتنظيمية التي تستثمر فيها المؤسسات الخدمية إن لم تترجم بشكل مباشر وملموس إلى إدراك إيجابي لدى المستهلك النهائي. يقف الفكر التسويقي المعاصر أمام مفارقة حرجة؛ ففي حين تتطلب هندسة الخدمات المخصصة استنزافا مستمرا لبيانات العميل، يفرض هذا الاستنزاف حالة من التوجس الدائم لديه. هنا يتدخل الأمن السيبراني ليلعب دور الوسيط السيكولوجي والتجاري الذي يذيب هذه المخاوف، محولا الجدران البرمجية المعقدة إلى جسور متينة تبني عليها المنظمة علاقاتها التبادلية، ومؤسسا لبيئة افتراضية تتسيد فيها الثقة كعملة بديلة وأصل استراتيجي غير ملموس.

أولاً: تعزيز الشعور بالأمان الرقمي.

ترتكز ديناميكية التفاعل في اقتصاد الخدمات بالدرجة الأولى على الإدراك النفسي للمخاطر المحتملة، حيث يتعامل المستهلك مع بيئة لا ملموسة تفتقر إلى الضمانات المادية التقليدية. يولد هذا الانكشاف الافتراضي ظاهرة سلوكية عميقة تعرف بالقلق الرقمي، وهي حالة من الترقب والشك تتملك العميل عند مطالبته بمشاركة معرفاته الشخصية أو بياناته البنكية لإتمام أي معاملة. ينبع هذا القلق من وعي المستهلك المعاصر بأن بصمته الرقمية عرضة للانتهاك والسرقة من قبل أطراف مجهولة، وهو ما يدفعه إلى تبني آليات دفاعية تتمثل في الإحجام عن الشراء أو تقديم بيانات مغلوطة تحمي خصوصيته. يعمل الأمن السيبراني الفعال على تفكيك هذه الحالة النفسية الدفاعية من خلال تقديم ضمانات تقنية قاطعة تحيد هذا القلق وتحوله إلى شعور مستدام بالأمان.[1]

تتأسس آلية تعزيز هذا الشعور بالأمان على ما يصطلح عليه أكاديميا بحسابات الخصوصية، وهو نموذج تحليلي يفسر السلوك الاستهلاكي بناء على موازنة دقيقة يجريها العميل بين المنافع التي سيجنيها من الخدمة، وبين حجم المخاطر المرتبطة بتقديم بياناته. تتدخل منظومة الأمن السيبراني بشكل حاسم

[1] . Khoa, B. T., Huynh, T. T., How do customer anxiety levels impact relationship marketing in electronic commerce?, Cogent Business & Management, Issue 1, Volume 9, Taylor & Francis, 2022, p. 5.

لترجيح كفة هذه المعادلة لصالح المنظمة، فعندما يدرك العميل أن المؤسسة تطبق بروتوكولات تشفير معقدة وتخضع لسياسات أمنية صارمة تمنع تسرب معلوماته حتى للموظفين غير المصرح لهم، تنخفض التكلفة النفسية والمخاطر المدركة لديه بشكل درامي. يسمح هذا الانخفاض في تقدير الخطر للمستهلك بتجاوز حاجز التردد والموافقة الطوعية على مشاركة أدق تفاصيل حياته وتفضيلاته، مقتنعا بأن العائد من هذه المشاركة سيكون خدمة فردية متفوقة تتم في بيئة محصنة لا تهدد استقراره المالي أو الاجتماعي[1].

يأخذ هذا الشعور بالأمان أبعادا عملية واضحة عندما تتبنى المؤسسات سياسة الشفافية في عرض إمكاناتها الأمنية. لم يعد إخفاء الإجراءات الدفاعية في الغرف الخلفية للإدارة مجديا، بل اتجهت المنظمات نحو إبراز المؤشرات المرئية للأمان، مثل شهادات التوثيق الرقمي، وعلامات التشفير، وبروتوكولات المصادقة الثنائية، كأدوات طمأنة مباشرة. تعمل هذه الإشارات البصرية على رسملة الجهد التقني، حيث تقرأ من قبل المستهلك كدليل قاطع على نضج المؤسسة واحترامها لسيادة العميل على بياناته. إن التزام المنظمة بتوضيح طبيعة البيانات المجموعة وكيفية تسييجها ضد الاختراق يبني عقدا نفسيا متينا يتجاوز حدود الصفقة اللحظية، ليؤسس لولاء إلكتروني عميق يرتكز على اليقين بأن الكيان الخدمي يمتلك القدرة التكنولوجية والنية الأخلاقية لحماية ظهر العميل في الفضاءات المفتوحة.[2]

تتعاظم حساسية هذا الدور في ظل الترسانة التشريعية الحديثة التي تفرض على المؤسسات حتمية الامتثال للقواعد القانونية الخاصة بحماية المعطيات.

إن قدرة المنظمة على استيعاب وتطبيق متطلبات القوانين الوطنية، كالقواعد الصارمة التي سنها المشرع الجزائري، تعكس نضجا حوكميا يبعث برسائل طمأنة بالغة القوة. فحين يلمس المستهلك أن حماية بياناته ليست مجرد ممارسة تقنية طوعية قد تتخلى عنها المؤسسة في أي لحظة، بل هي التزام قانوني سيادي تراقبه هيئات عليا، فإن شعوره بالأمان يرتقي إلى مستويات غير مسبوقة.[3]

ثانياً: الأمن السيبراني كميزة تنافسية تسويقية.

يفرض احتدام المنافسة في اقتصاد المعرفة وتطابق البدائل الخدمية المتاحة أمام المستهلك، ضرورة البحث عن محددات تفضيل استراتيجية تخرج المنظمة من دائرة التنافس السعري المدمر. وقد أفرزت التحولات التكنولوجية واقعا تشغيليا جديدا تحول بموجبه الانضباط السيبراني من مجرد التزام دفاعي

[1] Beke, F. T ,وآخرون, .Consumers privacy calculus: The PRICAL index development and validation, International Journal of Research in Marketing, Issue 1, Volume 39, Elsevier, 2021, p. 20.

[2] . Singh, N. et al., An analysis of consumer trusting beliefs towards the use of e-commerce platforms, Humanities and Social Sciences Communications, Issue 1, Volume 11, Springer Nature, 2024, p. 12.

[3] جمال زمورة، عيسى ليلى, أهمية حوكمة الأمن السيبراني لضمان تحول رقمي آمن للخدمات العمومية في الجزائر, مجلة البحوث الاقتصادية المتقدمة, العدد 02, المجلد 07, جامعة محمد خيضر بسكرة، الجزائر, 2022, ص 418.

وعبء مالي يقع على عاتق أقسام الدعم التقني، إلى أداة تسويقية هجومية وأصل تجاري ينتج ميزة تنافسية مستدامة. يبني المسوقون اليوم حملاتهم الترويجية وقراراتهم التموقعية على أساس الموثوقية الرقمية، مستغلين تصاعد الوعي المجتمعي بمخاطر الاختراقات وتفضيل شريحة واسعة من السوق التعامل مع الكيانات التي تثبت مناعتها ضد تسريب المعطيات.

تكتسي هذه الميزة التنافسية طابعا حاسما عند قراءة الإحصائيات المرتبطة بالسلوك الشرائي المعاصر، حيث تؤكد الدراسات الاستقصائية لتوجهات السوق أن الغالبية الساحقة من المستهلكين تشترط توافر الثقة المطلقة في العلامة التجارية قبل الإقدام على أي تعاقد رقمي، بل إن نسبة كبيرة منهم تبدي استعدادا فعليا لدفع هوامش سعرية إضافية مقابل الحصول على خدمات من منظمات تمتلك سجلا أمنيا نظيفا ولا تساوم على قدسية بيانات عملائها. يمنح هذا التفوق الأمني المؤسسة سلطة احتكارية ناعمة، حيث يرتفع حاجز الانتقال لدى العميل الراضي الذي يفضل البقاء ضمن بيئة محصنة ومألوفة بدلا من المخاطرة بالانتقال نحو منافس يقدم خدمة أرخص لكنه يفتقر إلى بنية تحتية قادرة على درء هجمات برمجيات الفدية أو التصيد الاحتيالي.[1]

يمتد الأثر الاقتصادي لهذه الميزة التنافسية ليشمل القدرة على حماية الحصة السوقية من التآكل السريع الذي يعقب عادة الحوادث الأمنية. في البيئات الخدمية الهشة، يكفي حدوث اختراق واحد وتسريب محدود لسجلات المشترين ليدمر عقودا من البناء التسويقي. يقوم المستهلكون المتضررون بردود فعل عقابية فورية تتمثل في الهجرة الجماعية نحو المنافسين ونشر تقييمات سلبية لاذعة عبر آليات الكلمة المنطوقة إلكترونيا، مما يشل قدرة المنظمة المخترقة على استقطاب عملاء جدد. في المقابل، تستحوذ المؤسسة التي تستثمر بكثافة في المرونة السيبرانية وتدريب قواها العاملة على حصص هؤلاء المنافسين المتعثرين، معززة بذلك موقعها القيادي في السوق كملاذ آمن جاذب للاستثمارات والتبادلات عالية الحساسية.[2]

يتطلب الاستثمار التسويقي للأمن السيبراني صياغة سياسات اتصالية ذكية تدمج التفوق التقني ضمن الهوية البصرية والمؤسسية للعلامة التجارية. لا يقتصر الأمر على امتلاك الجدران النارية، بل يمتد إلى قدرة إدارة التسويق على صياغة رسائل موجهة تخاطب العقل الباطن للعميل، وتؤكد له أن الاستثمار في خوارزميات التشفير هو في جوهره استثمار في احترام كيانه وحريته. هذا التطابق التام بين الوعود الترويجية والأداء التشغيلي المحكم يفرز حالة من الرضا العميق، حيث تتطابق التوقعات الأمنية المسبقة مع مستوى الجودة المدركة أثناء تلقي الخدمة وبعدها.

تتأكد هذه الحقيقة الاستراتيجية من خلال الطرح المنهجي الذي يربط بين الأمن القومي للمعلومات والمردودية الاقتصادية، حيث أصبحت كفاءة المنظومات الدفاعية معيارا يصنف على أساسه نضج الدول

[1] بن مويزة أحمد, مرجع سبق ذكره, ص 296.

[2] طويطي مصطفى، بوداود بومدين, مرجع سبق ذكره, ص 115.

والشركات على حد سواء. إن المؤسسات التي تنجح في مواءمة طموحاتها التسويقية التوسعية مع بروتوكولات حماية صارمة، هي وحدها القادرة على البقاء في صدارة المشهد، محولة التهديدات المعقدة في الفضاء الافتراضي إلى فرص استثنائية لإثبات الكفاءة، وتعزيز الولاء، وترسيخ صورة ذهنية لا تقبل المنافسة.[1]

يستنتج مما سبق بناء على تحليل معمق، أن الأمن السيبراني قد غادر مربعه التقني البحت ليحتل مركز القلب في صناعة القرار التسويقي. إن قدرة الخوارزميات وبرامج التدريب على درء الاختراقات هي المولد الحصري للثقة التي تبقي على ولاء العملاء وتدفعهم لمشاركة بياناتهم الطوعية. غير أن هذه الميزة الإيجابية تضعنا أمام حتمية دراسة الوجه الآخر للمعادلة؛ فماذا يحدث للكيان التسويقي والاقتصادي للمؤسسة عندما تنهار هذه الدفاعات وينجح المخترقون في استنزاف سجلات الزبائن؟ هذا ما يستوجب منا تحليله بدقة في المطلب الموالي.

المطلب الثالث: الانعكاسات التسويقية لفعالية حماية بيانات العملاء

تتجاوز فعالية الأمن السيبراني في بيئة الأعمال المعاصرة حدود الحماية التقنية الصرفة للبنى التحتية، لتفرز انعكاسات تسويقية عميقة تعيد تشكيل طبيعة العلاقة التبادلية بين المنظمة والعميل. لم يعد ينظر إلى الاستثمار في الجدران النارية وبروتوكولات التشفير على أنه مجرد عبء مالي تفرضه إدارات تكنولوجيا المعلومات لدرء المخاطر، بل تحول في الفكر الاستراتيجي الحديث إلى أصل تجاري غير ملموس ومولد مباشر للقيمة المضافة. تنطلق هذه المقاربة من حقيقة مفادها أن المستهلك الرقمي يواجه حالة مستمرة من الانكشاف الافتراضي، حيث تتطلب هندسة الخدمات المخصصة استنزافا دقيقا لمعطياته الشخصية والمالية. وأمام هذا الواقع، تتبلور فعالية التدابير الأمنية كأداة تسويقية هجومية تخفف من حدة القلق الرقمي، وتمنح المؤسسة قدرة فائقة على التموقع الاستراتيجي في أسواق تتسم بتطابق البدائل واحتدام المنافسة.

تتجلى أولى الانعكاسات وأكثرها تأثيرا في قدرة الأمن السيبراني على رفع القيمة المدركة للعلامة التجارية وتكريس الموثوقية الرقمية كمعيار أساسي للمفاضلة. في ظل اقتصاد الخدمات الذي يفتقر إلى الخصائص المادية الملموسة التي يمكن للزبون تقييمها قبل اتخاذ قرار التعاقد، تتحول الإشارات البصرية والتقنية الدالة على الأمان إلى بديل ملموس ومؤشر حاسم لجودة الخدمة. عندما تنجح المنظمة في استعراض كفاءتها السيبرانية، من خلال إبراز شهادات التوثيق الرقمي واعتماد آليات المصادقة المعقدة، فإنها ترسل رسائل سيكولوجية عميقة للمستهلك تفيد باحترامها لسيادته على بياناته. هذا الإدراك الإيجابي يترجم فورا إلى ما يعرف في الأدبيات التسويقية بتخفيض التكلفة النفسية المرتبطة باستهلاك الخدمة.

[1] يوسف بوغرارة, الأمن السيبراني: الإستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبراني, أطروحة دكتوراه, تخصص القانون العام, كلية الحقوق والعلوم السياسية، جامعة مستغانم، الجزائر, 2017, ص 33.

فالمنظمات التي تتموضع في السوق ككيانات آمنة وموثوقة على صعيد حماية الخصوصية، تكتسب ميزة تنافسية حاسمة تسمح لها باحتكار شريحة واسعة من العملاء الذين يضعون أمن معطياتهم فوق كل اعتبار، بل ويكونون على استعداد تام لدفع هوامش سعرية إضافية مقابل الاستفادة من بيئة استهلاكية محصنة لا تهدد استقرارهم المالي أو الاجتماعي.[1]

يمتد الأثر التسويقي لصرامة الإجراءات الأمنية ليحكم جودة وحجم البيانات التي يمكن للإدارة التسويقية تجميعها من السوق، وهو ما يفسر عبر نظرية حسابات الخصوصية. يرتكز هذا النموذج التحليلي على موازنة دقيقة يجريها العميل في عقله الباطن بين المنافع الخدمية التي سيجنيها، وبين حجم المخاطر الأمنية المرتبطة بتسليم معطياته. يميل المستهلكون الذين تساورهم شكوك حول قدرة المؤسسة على ردع الاختراقات إلى ترجيح كفة الخطر، ويتبنون سلوكيات دفاعية حادة تتمثل إما في الامتناع الكلي عن التفاعل الرقمي، أو اللجوء إلى تضليل خوارزميات التتبع عبر تقديم بيانات ديموغرافية وسلوكية مغلوطة. هذا التشويه العمدي للمدخلات يضرب صميم العمل التسويقي ويعمي بصيرة متخذ القرار، مما يؤدي إلى تصميم حملات إعلانية فاشلة وتطوير خدمات لا تتطابق مع الواقع. على النقيض من ذلك، أثبتت الدراسات الميدانية أن المستهلك الذي يثق في البنية السيبرانية للمؤسسة يميل إلى التخلي عن حذره، ويصبح أكثر انفتاحا واستعدادا لتقديم معلوماته الشخصية الدقيقة طواعية. ينتج عن هذا الاستسلام الطوعي تدفق معلوماتي نقي وعالي الجودة، يمنح المسوقين القدرة على استخلاص أنماط استهلاكية صحيحة، وتصميم خدمات مخصصة تلبي أدق التطلعات الفردية، وهو ما يرفع من معدلات التحويل ويعظم العائد على الاستثمار في الأنشطة الترويجية.

تأخذ هذه الانعكاسات طابعا دفاعيا ووقائيا عندما يتعلق الأمر بإدارة السمعة المؤسسية وتوجيه الكلمة المنطوقة إلكترونيا. تمثل حوادث خرق البيانات تسونامي حقيقيا يعصف بالجهود التسويقية المتراكمة لسنوات، حيث لا تقتصر تداعيات الفشل الأمني على التعويضات المالية أو الغرامات القانونية، بل تتسرب بسرعة فائقة لتدمر الصورة الذهنية للعلامة التجارية في أذهان الجمهور. إن المتتبع للسلوك الاستهلاكي يدرك أن تداعيات تسريب السجلات الشخصية تغير الأنماط التفاعلية للمتضررين بشكل جذري ودرامي، حيث تشير الإحصائيات الدقيقة إلى أن ما يقارب سبعين بالمائة من المستهلكين يتخذون قرارا قطعيا بالتوقف النهائي عن التسوق أو التعامل مع العلامة التجارية التي تعرضت لحادث أمني أدى إلى كشف بياناتهم[2]. ولا يقف نزيف الحصة السوقية عند هذا الحد، بل يتضخم بفعل قوة المجتمعات الافتراضية وشبكات التواصل الاجتماعي، حيث يميل أكثر من خمسة وثمانين بالمائة من المستهلكين المحبطين إلى مشاركة تجاربهم السلبية المتعلقة بانعدام الأمن مع دوائرهم الاجتماعية. يحيد هذا الضخ

[1] . H. Jeff Smithet al., Information Privacy Research: An Interdisciplinary Review ،MIS Quarterly, vol 04, Management Information Systems Research Center, 2011, p999.

[2] Hardeep singh وآخرون، مرجع سبق ذكره، ص 2104.

الهائل من المراجعات السلبية مفعول كافة الميزانيات المرصودة للحملات الإعلانية، ويجعل من استقطاب عملاء جدد عملية شبه مستحيلة. وعليه، فإن الفعالية الحقيقية للأمن السيبراني تكمن في قدرته على حماية الأصول السمعية للمنظمة، ومنع تحولها إلى مادة للتشهير الرقمي، محتفظا بصورتها ككيان صلب يحترم قدسية التزاماته.

من منظور بناء العلاقات طويلة الأجل، يخلق الالتزام الأمني الصارم حواجز تحول عالية تعيق تسرب العملاء نحو المنافسين. إن الشعور المستدام بالأمان يولد حالة من الاستقرار النفسي لدى الزبون، مما يجعله مقاوما للإغراءات الترويجية والعروض السعرية التي يقدمها المنافسون الجدد في السوق. يفضل المستهلك العقلاني البقاء ضمن بيئة رقمية مختبرة ومألوفة أثبتت مناعتها ضد هجمات التصيد وبرمجيات الفدية، عوضا عن المخاطرة بنقل سجلاته المالية ومعرفاته الحساسة إلى مؤسسة أخرى قد تفتقر إلى النضج السيبراني اللازم. يتحول هذا الارتياح تدريجيا إلى ولاء سلوكي وعاطفي عميق، حيث تصبح المنظمة هي الخيار الأوحد والحصري لتلبية الحاجات الاستهلاكية، وهو ما يجسد الغاية القصوى من استراتيجيات التسويق بالعلاقات التي تبحث عن استدامة التدفقات النقدية وخفض تكاليف الاستقطاب المستمر.[1]

يتأكد من خلال هذا الرصد التحليلي أن الاستثمار في أدوات الحماية الرقمية يتطابق تماما مع الاستثمار في نمو المنظمة وتوسعها التجاري. إن فعالية الأمن السيبراني لا تقاس فقط بعدد الهجمات التي تم إحباطها، بل بحجم الثقة التي تم ترسيخها، ونوعية البيانات التي تم استقطابها، والسمعة التي تم تحصينها. إنها باختصار الآلية التشغيلية الوحيدة القادرة على تحويل بيئة المخاطر المفتوحة إلى مساحة آمنة ومربحة، تضمن للمؤسسة الخدمية التفوق، وللعميل الطمأنينة الكاملة.

[1] . Chris Halliburton, The Role of Trust in Consumer Relationships ESCP Europe Business School, 2010, p 10.

خلاصة الفصل الثاني

تجسد مسارات هذا الفصل حقيقة تشغيلية واستراتيجية قاطعة تتمثل في أن الأمن السيبراني قد تجاوز تموضعه التقليدي كأداة تقنية بحتة تقبع في الغرف الخلفية لإدارة الأنظمة، ليحتل صدارة القرار التسويقي والقانوني داخل المؤسسات الخدمية. أثبت التحليل المنهجي لآليات الحماية سواء كانت برمجيات تشفير معقدة أو سياسات إدارية لضبط السلوك البشري أن الغاية لا تقف عند حدود صد الاختراقات ومنع تسريب بيانات العملاء، بل تتعداها إلى بناء جدار ثقة متين يربط المنظمة بمحيطها الاستهلاكي.

في بيئة رقمية تتسم بالانكشاف والهشاشة يتحول الانضباط الأمني إلى أصل تجاري غير ملموس وميزة تنافسية حاسمة. العميل المعاصر يبني قراره التعاقدي بناء على تقدير دقيق للمخاطر والمؤسسة التي تفشل في حماية سرية وسلامة بياناته تفقد مبرر وجودها في السوق وتعرض نفسها لمساءلات قانونية صارمة تعصف بكيانها المالي والسمعي. بالمقابل تترجم المرونة السيبرانية والامتثال لبروتوكولات الحماية إلى رسائل طمأنة سيكولوجية تخفض من القلق الرقمي وتدفع المستهلك نحو تقديم معطيات عالية الجودة طواعية، مما يمنح الإدارة التسويقية قدرة استباقية على تخصيص الخدمات ورفع معدلات الولاء والاحتفاظ بالعملاء.

نستنتج بناء على هذا الطرح أن الفعالية الحقيقية للأمن السيبراني تكمن في تلاحمه العضوي مع الفلسفة التسويقية. الجدران النارية وأنظمة اكتشاف التسلل هي في جوهرها أدوات لحراسة السمعة المؤسسية وتأمين التدفقات النقدية. يفرض هذا الواقع تحولا حتميا في الثقافة التنظيمية، حيث يصبح كل موظف وكل خوارزمية جزءا من درع شامل يضمن استدامة العلاقة مع الزبون ويحول التهديدات الافتراضية إلى فرص فعلية لترسيخ السيادة الرقمية والتميز الخدماتي.

الفصل الثالث:

فعالية الامن السيبراني في حماية بيانات عملاء وكالة اتصالات الجزائر - تبسة-

المبحث الأول: تقديم عام لمؤسسة اتصالات الجزائر

في أدبيات الإدارة الاستراتيجية والنظرية التنظيمية المعاصرة، يُنظر إلى المؤسسة على أنها نظام مفتوح يتفاعل باستمرار مع بيئته الخارجية، يؤثر فيها ويتأثر بها، ومن هذا المنطلق تلعب المؤسسات الخدماتية الكبرى دورا استراتيجيا وحاسما في دفع عجلة التطور الاقتصادي والاجتماعي لأي بلد، وتعتبر بمثابة الشريان الذي يغذي باقي القطاعات الاقتصادية الأخرى .ومن منظور الباحث في علوم التسيير، لا يمكن الشروع في دراسة أداء مؤسسة ما، أو تقييم كفاءتها التنظيمية، دون أن يسبق ذلك فهم عميق ودقيق لهويتها، طبيعة نشاطها، ومسارها التطوري.

إن هذا المبحث مُخصص للقيام بتشخيص استراتيجي وصفي لمؤسسة "اتصالات الجزائر"، حيث سنقوم بإعطاء نظرة عامة ومفصلة عن هذا الكيان الاقتصادي العملاق .يسعى هذا التقديم إلى إبراز الجوانب الهيكلية والتنظيمية للمؤسسة، انطلاقا من فهم جذورها التاريخية والظروف التي أدت إلى نشأتها، مرورا بتحديد مهامها الأساسية والدور الذي تلعبه في النسيج الاقتصادي، وصولا إلى استعراض شبكة فروعها واستراتيجياتها التي مكنتها من التموقع كفاعل رئيسي ومهيمن في السوق الجزائرية .إن الإحاطة الشاملة بهذه الأبعاد تُعد خطوة منهجية ضرورية لتأطير الدراسة وتوفير الأرضية المعرفية الخصبة لفهم كيف تتفاعل المؤسسة مع متغيرات بحثنا بشكل دقيق.

المطلب الأول: نبذة تاريخية عن نشأة المؤسسة

إن علوم الإدارة تُعلمنا أن التاريخ المؤسسي ليس مجرد سرد زمني جاف للأحداث والأرقام، بل هو أداة تحليلية بالغة الأهمية لفهم "الجينات التنظيمية" والثقافة المؤسسية التي تحكم سلوك الكيان الاقتصادي وتوجه قراراته في الحاضر. إن دراسة نشأة المؤسسات، وخاصة تلك التي تنبثق من تحولات هيكلية كبرى في اقتصاديات الدول، تكشف لنا بوضوح حجم التحديات التي واجهتها وكيفية تفعيلها لاستراتيجيات التكيف مع معطيات المحيط المتغيرة.

بالنسبة لقطاع الاتصالات في الجزائر، فقد شهد تحولات مفصلية استجابة لمتطلبات العولمة، وثورة تكنولوجيا المعلومات، وتوجهات اقتصاد السوق، ولفهم المكانة الريادية التي تحتلها "اتصالات الجزائر" اليوم، وتفسير سلوكها التنظيمي الحالي، يتحتم علينا كطلبة وباحثين تتبع جذورها التاريخية بعناية فائقة، وتحليل الدوافع التكنولوجية والاقتصادية والتشريعية التي فرضت على صانع القرار في الجزائر إعادة هيكلة قطاع البريد والمواصلات الكلاسيكي، وتأسيس كيانات اقتصادية جديدة تتسم بالمرونة، والفاعلية، والقدرة على المنافسة في بيئة شديدة التعقيد .

أولا: تأسيس اتصالات الجزائر

إن الحديث عن التأسيس الفعلي والنشأة المؤسسية لمجمع "اتصالات الجزائر" يقودنا حتما إلى رصد التحولات العميقة وبرامج إعادة الهيكلة التي باشرتها الدولة الجزائرية منذ أواخر التسعينيات، وتحديدا منذ عام 1999، في قطاع البريد والمواصلات، لقد فرضت التحديات التكنولوجية العالمية المتسارعة، والنمو الهائل في الطلب على خدمات الاتصال، حتمية عصرنة القطاع وتكييفه مع مستجدات الاقتصاد العالمي المفتوح.

وقد تُوّجت هذه الجهود الإصلاحية الهيكلية بخطوة تشريعية استراتيجية بالغة الأهمية، تمثلت في صدور القانون رقم 2000/03 المؤرخ في 05 أوت 2000، والذي يُعد بمثابة حجر الأساس ونقطة التحول الجذرية في تاريخ إدارة الاتصالات الجزائرية، وجاء هذا القانون التاريخي ليُحدث قطيعة مع الماضي، ويُنهي حقبة طويلة من الاحتكار المطلق للدولة على نشاطات البريد والمواصلات، مؤسسا لمبدأ إداري وتنظيمي حديث وفعال يتمثل في "الفصل العضوي والوظيفي" بين نشاط التنظيم والضبط من جهة، ونشاط الاستغلال التجاري وتسيير الشبكات من جهة أخرى.

وتجسيدا لهذا المبدأ الاستراتيجي على أرض الواقع، تم إنشاء سلطة ضبط مستقلة ماليا وإداريا تسهر على تنظيم السوق، كما تم تقسيم المهام التشغيلية على متعاملين اقتصاديين رئيسيين: الأول خُصص للنشاطات البريدية والخدمات المالية وهو مؤسسة "بريد الجزائر"، في حين برز المتعامل الثاني ككيان مخصص حصريا لإدارة وتطوير قطاع الاتصالات، وهو مؤسسة "اتصالات الجزائر."

ومن الناحية الرسمية والقانونية، أقرّ المجلس الوطني لمساهمة الدولة (CNEP) في 01 مارس 2001 قرارا بإنشاء مؤسسة اتصالات الجزائر كمؤسسة عمومية اقتصادية تسير بمنطق تجاري بحت .وقد اتخذت الشركة الشكل القانوني كشركة ذات أسهم SPA، تعود ملكية أسهمها بالكامل وبنسبة 100% للدولة الجزائرية، ولضمان انطلاقة اقتصادية قوية تليق بحجم الاستثمارات التكنولوجية المطلوبة في البنية التحتية، تم تزويد هذه المؤسسة بغطاء مالي متين، حيث تم تسجيلها في مركز السجل التجاري بتاريخ 11 ماي 2002 تحت الرقم B02.18083 وقد بدأت برأس مال أولي قدره 50.000.000.000 دينار جزائري (خمسون مليار دينار جزائري)، والذي ارتفع وتكيف لاحقا وفق القيود المحاسبية للمؤسسة ليبلغ 61.275.180.000 دينار جزائري، مما يعكس الرغبة الصارمة في توسيع قدراتها التمويلية والتنافسية.

وقد بدأت مؤسسة اتصالات الجزائر في مزاولة نشاطها الاقتصادي والتجاري الفعلي، والدخول رسميا إلى سوق العمل في 01 جانفي 2003 .وقد حملت هذه المؤسسة الفتية على عاتقها مسؤولية تاريخية كبرى

تتمثل في تطوير، وتحديث، ورقمنة شبكة الاتصالات في الجزائر، والانتقال بها نهائيا من التسيير الإداري الحكومي البيروقراطي إلى التسيير الاقتصادي المرن والمستقل عن وصاية وزارة البريد.

وفي إطار سياسة الانفتاح التدريجي نحو اقتصاد السوق، شهد شهر جوان من عام 2003 بيع رخصة الإقامة واستغلال شبكة الهاتف النقال وشبكة الربط المحلي في المناطق الريفية والحضرية، ليتوسع هذا الانفتاح الاستراتيجي لاحقا ويشمل الدارات الدولية، مما أدى إلى جعل سوق الاتصالات في الجزائر سوقا مفتوحة تماما للمنافسة بحلول عام 2005، وذلك ضمن أطر تشريعية تحترم قواعد المنافسة الحرة ومبادئ الشفافية التامة.

اليوم، وبفضل مسارها التأسيسي الصلب ورؤيتها التوسعية، أضحت اتصالات الجزائر تمارس نشاطها عبر انتشار جغرافي واسع يغطي كافة التراب الوطني من خلال 48 وحدة عملية متكاملة .وهي تعمل جاهدة على تقديم تشكيلة متنوعة من الخدمات والمنتجات الاستراتيجية ذات الطابع الطبيعي والمعنوي، مسطرة أمامها جملة من الأهداف الحيوية المتمثلة أساسا في: تحقيق الفعالية التشغيلية، ضمان الجودة العالية في تقديم الخدمات للمواطنين والمؤسسات، وتحقيق المردودية الاقتصادية التي تضمن لها البقاء، والنمو، والتطور كعصب محوري ورائد لا غنى عنه في ميدان تكنولوجيا الاتصال الحديثة على المستوى الوطني.

ثانيا: الإطار القانوني لمؤسسة اتصالات الجزائر

في أدبيات علوم التسيير والإدارة الاستراتيجية، لا يُنظر إلى الإطار القانوني لأي مؤسسة اقتصادية على أنه مجرد مجموعة من النصوص والتشريعات الجامدة، بل يُعتبر بمثابة "الحمض النووي التنظيمي " (Organizational DNA) الذي يحدد هوية المؤسسة، ونطاق صلاحياتها، وهامش المرونة المتاح لها في اتخاذ القرارات الاستراتيجية والتشغيلية. إن انتقال أي كيان من تسيير حكومي إداري بيروقراطي خاضع للوصاية المباشرة للوزارات، إلى كيان اقتصادي يعمل بمنطق تجاري وتنافسي، يستوجب بالضرورة إحداث قطيعة قانونية مع الماضي. هذا التحول القانوني هو الذي يمنح المؤسسة الاستقلالية المالية والإدارية التي تسمح لها بالاستجابة السريعة لتقلبات السوق، وتطوير ميزتها التنافسية، وإدارة مواردها البشرية والمالية بكفاءة عالية. وفي حالة "مؤسسة اتصالات الجزائر"، كان الغطاء القانوني هو نقطة الانطلاق الجوهرية التي مهدت الطريق لتحرير قطاع الاتصالات في الجزائر، ونقله من بيئة الاحتكار المطلق إلى بيئة اقتصاد السوق والانفتاح التنافسي.

1. المخاض التشريعي وقانون 2000/03 (نقطة التحول الاستراتيجي):

لقد جاءت نشأة مؤسسة اتصالات الجزائر كاستجابة حتمية للتحولات التكنولوجية العميقة التي شهدها العالم، وكجزء من برنامج إصلاحي شامل ومكثف باشرته الدولة الجزائرية لهيكلة قطاع الاتصالات وتحديثه بما يتوافق مع المعايير الدولية المعاصرة. لقد تبلور هذا المسار الإصلاحي تشريعيا من خلال صدور القانون التاريخي رقم 2000/03 المؤرخ في 05 أوت 2000.

من المنظور الإداري والتنظيمي، يُعد هذا القانون ثورة حقيقية في طريقة إدارة المرافق العامة في الجزائر؛ فقد نص بشكل صريح ومباشر على إنهاء احتكار الدولة المطلق على نشاطات البريد والمواصلات، وأسس لمبدأ "الفصل العضوي والوظيفي ."هذا المبدأ الاستراتيجي أدى إلى تقسيم قطاع البريد والمواصلات الكلاسيكي إلى قسمين منفصلين ومستقلين تماما عن بعضهما البعض: الأول هو "بريد الجزائر" الذي كُلف بإدارة النشاطات والخدمات البريدية والمالية، والثاني هو مؤسسة "اتصالات الجزائر (Algérie Télécom) " التي أُسندت إليها مهام استغلال وتسيير وتطوير شبكات الاتصالات. إن هذا التقسيم القانوني يُترجم مبدأ "التخصص" في علوم التسيير، حيث يُسمح لكل كيان بالتركيز حصريا على كفاءته الجوهرية Core Competence، مما يعزز من جودة الخدمات ويرفع من معدلات الأداء والإنتاجية. بموجب هذا القانون، حملت مؤسسة اتصالات الجزائر على عاتقها مسؤولية وطنية كبرى تتمثل في تطوير شبكة الاتصالات وتحديثها باستقلالية تامة في التسيير عن الإدارة المركزية لوزارة البريد.

2. التأسيس المؤسسي والطبيعة القانونية (شركة ذات أسهم)

استكمالا للمسار التشريعي الذي رسمه قانون 2000/03، كان لزاما إيجاد الصيغة القانونية والمؤسسية التي ستعمل من خلالها اتصالات الجزائر في الميدان الاقتصادي. وبناء على ذلك، أصدر المجلس الوطني لمساهمة الدولة (CNEP) قرارا حاسما بتاريخ 01 مارس 2001، ينص رسميا على إنشاء هذه المؤسسة العمومية الاقتصادية تحت اسم "اتصالات الجزائر."

من الناحية القانونية البحتة، تم تأسيس اتصالات الجزائر في شكل "شركة ذات أسهم – SPA) " Société Par Actions) إن اختيار هذا الشكل القانوني التجاري بالذات يحمل دلالات تسييرية عميقة؛ فشركة المساهمة تضمن وجود هياكل حوكمة حديثة (مثل مجلس الإدارة والجمعية العامة)، وتوفر مرونة فائقة في الإدارة المالية، وتسمح للمؤسسة بالعمل وفقا لقواعد القانون التجاري بدلا من القانون الإداري العام. ورغم اتخاذها لهذا الطابع التجاري المرن، إلا أن المشرع حافظ على السيادة الوطنية في هذا القطاع الحساس، حيث تعتبر مؤسسة اتصالات الجزائر شركة مملوكة بالكامل للدولة الجزائرية، وتعود ملكية أسهمها

بنسبة 100% للدولة. هذا التزاوج القانوني بين "الملكية العمومية المطلقة" و"آليات التسيير التجاري الخاص" أتاح للمؤسسة الدخول بقوة في سوق الخدمات السلكية واللاسلكية، مع الحفاظ على دورها التنموي والسيادي.

3. الغطاء المالي والتسجيل التجاري (متطلبات البنية التحتية)

في علم الإدارة المالية، يُعتبر رأس المال التأسيسي بمثابة شريان الحياة الذي يضمن قدرة المؤسسة على اقتناء التكنولوجيا، وبناء البنى التحتية، وتغطية النفقات الاستثمارية الرأسمالية الضخمة(CAPEX) ونظرا لطبيعة قطاع الاتصالات الذي يتطلب استثمارات هيكلية هائلة في الكابلات، والمقاسم، والألياف البصرية، فقد تم تزويد الكيان القانوني الجديد بغطاء مالي متين جدا يتناسب مع حجم المهام الموكلة إليه.

تم تسجيل مؤسسة اتصالات الجزائر رسميا في مركز السجل التجاري بتاريخ 11 ماي 2002 .وقد قُيدت تحت رقم السجل التجاري 18083 B02، والذي يُشار إليه تنظيميا أيضا بالرقم(B02/0018083) لتجسيد الانطلاقة القوية، مُنحت المؤسسة في البداية رأس مال اجتماعي ضخم قُدر بـ 50.000.000.000 دينار جزائري (خمسون مليار دينار جزائري) ومع تطور متطلبات المؤسسة وإعادة تقييم أصولها والتزاماتها لضمان تغطية كافة المشاريع الاستراتيجية والتوسعية، تم تحديد وضبط رأس مال الشركة لاحقا ليبلغ 61.275.180.000 دينار جزائري. إن هذا التأسيس المالي الصلب لا يخدم فقط الجانب المحاسبي، بل هو رسالة ثقة تسييرية وقانونية لكافة المتعاملين والموردين المحليين والدوليين بقدرة المؤسسة على الوفاء بالتزاماتها الاستثمارية طويلة الأجل.

4. الانطلاقة التشغيلية والانتشار الهيكلي على المستوى الوطني

بعد استكمال كافة الجوانب التشريعية والمالية والتنظيمية، تحولت اتصالات الجزائر من مجرد كيان قانوني على الورق إلى فاعل اقتصادي حيوي في السوق. حيث بدأت المؤسسة في مزاولة نشاطها الاقتصادي والتجاري الفعلي على أرض الواقع ابتداء من 01 جانفي 2003.

بفضل استقلاليتها القانونية والإدارية، تمكنت المؤسسة من بناء هيكل تنظيمي واسع الانتشار يغطي كافة أرجاء البلاد، حيث باتت تشمل وتدير 48 وحدة عملية موزعة بدقة على كامل التراب الوطني لضمان تقريب الإدارة من الزبون وتلبية احتياجاته. ومن خلال هذا الغطاء القانوني القوي، تقوم المؤسسة بتقديم تشكيلة واسعة ومتنوعة من المنتجات والخدمات ذات الطابع الطبيعي المادي والمعنوي، والتي تهدف في مجملها إلى تمكين الأفراد والمؤسسات من الولوج إلى أحدث تكنولوجيات الاتصال ونقل البيانات، وبالتالي المساهمة بشكل فعال في دفع عجلة التنمية الشاملة للاقتصاد الوطني.

ثالثا: خدمات مجمع اتصالات الجزائر

بصفتنا طلبة وباحثين في علوم التسيير، ندرك تماما أن بقاء أي مؤسسة اقتصادية ونموها في سوق شديدة التنافسية يعتمد بشكل جوهري على استراتيجية "تنويع محفظة المنتجات والخدمات Product) " (Portfolio Diversification إن المؤسسات الخدمية الرائدة لا تكتفي بتقديم خدمة واحدة، بل تسعى جاهدة لمحاصرة احتياجات الزبون من خلال تقديم حزم متكاملة من الخدمات ذات القيمة المضافة. وعندما نضع "مجمع اتصالات الجزائر" تحت المجهر التسويقي والتسييري، نجد أنه تبنى سياسة هجومية ذكية لتقديم مجموعة واسعة من المنتجات الخدمية، سواء ذات الطابع الطبيعي المادي أو المعنوي، لتشمل قطاعات الهاتف الثابت، الهاتف النقال، والإنترنت، فضلا عن تقديم حلول مبتكرة للمؤسسات والأفراد. وسنقوم فيما يلي بتشريح هذه الخدمات وتصنيفها تحليليا:

1. خدمات الهاتف الثابت (الأساس الكلاسيكي والخدمات ذات القيمة المضافة)

يُعد الهاتف الثابت النواة التاريخية لنشاط المؤسسة، حيث تعتمد اتصالات الجزائر على الشبكة الهاتفية المجمعة (RTC) التي تعتبر تقنية تسمح بالتحدث بين أكثر من متحدثين، وتزيد من قدرات التركيبات المكلفة بالأسلاك النحاسية في وقت واحد، ولتعظيم العوائد من هذه الشبكة الأساسية، لم تكتفِ المؤسسة بتوفير حرارة الاتصال فقط، بل طرحت باقة من الخدمات المضافة لتسهيل حياة الزبائن ورفع مستوى ولائهم، نذكر منها:

- **خدمة الدفع المسبق:** استراتيجية ممتازة تتيح للمشتركين إجراء المكالمات في أي وقت عبر رصيد استهلاكي باستخدام خطوط الهواتف العمومية.
- **إعلام بنداء في الانتظار:** خدمة تسييرية ذكية تمنع ضياع المكالمات المهمة، حيث تُعلم المشترك بوجود اتصال آخر عبر إشارة سمعية، مما يمنحه مرونة في تعليق المكالمة الأولى أو إنهائها لاستقبال المكالمة الجديدة.
- **النداء بدون ترقيم:** خدمة تحمل طابعا اجتماعيا وإنسانيا راقيا، حيث تسمح بالحصول على رقم مبرمج أوتوماتيكيا بمجرد رفع السماعة ومرور 5 ثوانٍ، وهي موجهة خصيصا للأطفال، الأشخاص المسنين، وذوي الاحتياجات الخاصة (كفاقدي البصر).
- **المحاضرة الثلاثية:(Conference Call)** وهي أداة إدارية فعالة جدا لقطاع الأعمال، حيث تسمح بربط ثلاثة مشتركين في نفس الوقت، مما يسهل عقد الاجتماعات عن بُعد ويقلل من تكاليف تنقل الإطارات.

- **تحويل النداء والترقيم المختصر:** لضمان الفعالية والسرعة، يمكن للمشترك تحويل مكالماته الواردة إلى رقم آخر، أو استبدال الأرقام الطويلة بأرقام مختصرة (من 1 إلى 8 أو 10 أرقام) لتجنب أخطاء التشكيل وربح الوقت.

- **أدوات الرقابة المالية (الفاتورة المفصلة وإقفال الاستعمال الدولي):** من منظور التسيير المالي للأسرة أو المؤسسة، توفر اتصالات الجزائر خدمة "الإقفال برمز سري" لمنع المكالمات الدولية المكلفة، بالإضافة إلى خدمة "الفاتورة المفصلة" التي تمنح الزبون قائمة دقيقة بكافة اتصالاته، مما يساعد في التسيير العقلاني للمصاريف الهاتفية والتحكم في الميزانية.

2. خدمات الهاتف النقال فرع موبيليس Mobilis

بصفتها فاعلا لا يُستهان به في مجال تكنولوجيا الاتصال، أسست اتصالات الجزائر فرعها "موبيليس" المتخصص في الهاتف الخلوي، والذي يرتكز على بنية تحتية قاعدية ضخمة تتجاوز 4200 محطة بث لاسلكي BTS ومن الناحية التجارية، تملك موبيليس شبكة تسويقية متطورة تتجاوز 85 وكالة تجارية وأكثر من 35,000 نقطة بيع معتمدة، لتخدم قاعدة زبائن تتخطى حاجز 10 ملايين مشترك. وقد ابتكرت موبيليس عروضا تسويقية متنوعة لتغطية كافة الشرائح السوقية، مثل (موبي كنترول، قوسطو، رسيمو، خدمات الجيل الثالث، والتعبئة الإلكترونية "أرسلي" ولعل من أبرز ابتكاراتها الاستراتيجية لغزو الأسواق الخارجية خدمة **الاتصال المباشر الوافد (DID – Direct Inward Dialing)** وهي خدمة تعتمد على أرقام افتراضية تم تفعيلها بالشراكة مع متعاملين أجانب، وتستهدف المغتربين في (أمريكا، كندا، وأوروبا) فمثلا، يمكن لجزائري مقيم في مونتريال بكندا الحصول على رقم هاتفي جزائري، مما يسمح لعائلته في الجزائر بالاتصال به بتسعيرة محلية مخفضة جدا (حوالي 4.50 دج للدقيقة)، حيث يتكفل المتعامل الأجنبي بتوفير التجهيزات لضمان نجاح العملية.

3. الهاتف الثابت اللاسلكي (WLL) وتكنولوجيا CDMA

في علوم العمليات، ندرك أن البنية التحتية السلكية قد تواجه عوائق جغرافية وتكاليف صيانة باهظة. كحل استراتيجي لتجاوز هذا التأخر في الكثافة الهاتفية، خاصة في المناطق الريفية، تبنت اتصالات الجزائر تكنولوجيا "الدائرة المحلية راديو(WLL) " بتقنيةEVDO CDMA 2000 . تتميز هذه التقنية بمرونة عالية، سرعة في الانتشار، وسهولة في الصيانة (خاصة في الشتاء) لأنها لا تعتمد على الخيوط والأعمدة، مما يضمن تدخلا سريعا لإصلاح الأعطاب، ويوفر جودة خدمات مضمونة ومكالمات مؤمنة. ومن خلال هذه التقنية، توفر المؤسسة خدمات الصوت، الفاكس، ونقل البيانات بسرعات تصل إلى 153.6 كيلوبايت/ثانية.

وللتحكم في هذا الاستهلاك، توفر المؤسسة بطاقات تعبئة مثل بطاقة "أمال" (بفئات 50، 100، و200 دج) التي تسمح للزبون بمراقبة رصيده بدقة

4. خدمات الإنترنت ونقل البيانات (فرع جوابDjaweb):

إن البيانات هي نفط العصر الحديث، ولذلك أنشأت المؤسسة فرع "جواب" الذي أخذ على عاتقه تطوير المجتمع المعلوماتي في الجزائر من خلال تيسير الولوج إلى الإنترنت ذات التدفق العالي. يوفر هذا الفرع عروض "أنيس بلوس (Anis Plus) "المبنية على تكنولوجيا الجيل الجديد(NGN) ومن منطلق التجزئة السوقيةMarket Segmentation))، قسمت المؤسسة عروضها لتلائم فئات محددة:

- **للخواص والمهنيين الأحرار:** عروض (Anis Home) و (Anis Elite) بتدفقات تتراوح بين 512 كيلوبايت/ثانية وتصل حتى 8 ميغابايت.
- **للمؤسسات والمحترفين:** عرض (Anis Pro) الذي يوفر سرعات إنترنت فائقة تتراوح من 1 ميغابايت إلى 20 ميغابايت، مما يعزز من كفاءة هذه المؤسسات.

5. العروض المبتكرة واستراتيجية استرجاع الديون عرض سهلي SEHELLI

من أروع الأمثلة التي يمكن دراستها كطلبة تسيير في مجال "إدارة الديون" و"التسويق الاسترجاعي" هو عرض "**سهلي** ."لقد عانت المؤسسة من مشكلة تراكم الديون وتزايد عدد الخطوط الأرضية المقطوعة وغير المستغلة. لمعالجة هذه المعضلة المزدوجة (ديون غير محصلة + فقدان الزبائن)، أطلقت المؤسسة هذا العرض الاستثنائي الموجه للزبائن الذين قُطعت خطوطهم لأكثر من 6 أشهر. تكمن عبقرية هذا العرض الإداري في أنه يوفر **بدائل مرنة للتسديد بالتقسيط**، ويمنح الزبون محفزات قوية تتمثل في:

- استعادة الخط تدريجيا (استقبال المكالمات كخطوة أولى).
- الحصول على بطاقة "أمال" مجانية بعد دفع القسط الأول.
- ربط الزبون باشتراك إنترنت عالي التدفق (ويفي) موازاة مع الدفع الجزئي. هذه الاستراتيجية حققت للمؤسسة أهدافا مالية وتجارية بالغة الأهمية تتمثل في: رفع رقم الأعمال، تقليص حظيرة الهواتف المعطلة، استرجاع الديون العالقة، وإبراز بُعد المواطنة والمسؤولية الاجتماعية للمؤسسة.

6. الاستثمارات الهيكلية والبنية القاعدية الكبرى

لضمان استدامة كل هذه الخدمات وجودتها، استثمر مجمع اتصالات الجزائر في بنى تحتية استراتيجية ذات بعد دولي ومحلي. فقد اعتمدت المؤسسة استراتيجية تقنية تتمثل في بناء شبكة اتصالات حديثة موزعة

ومتسلسلة بتقنية (DWDM – IP/MPLS) لضمان ربط جيد ومضمون إلى جانب ذلك، استثمرت المؤسسة في الكابل البحري للألياف البصرية (SEA NE WE4) الذي يربط الجزائر بأوروبا، ومشاريع الهاتف الثابت اللاسلكيCDMA–EVDO/WL))، وتوسعة شبكة الإنترنت الفضائية وعبر الأقمار الصناعية–WIMA) .WIFI)

المطلب الثاني: فروع واستراتيجيات مجمع اتصالات الجزائر

في أدبيات الإدارة الاستراتيجيةStrategic Management))، تلجأ المؤسسات الاقتصادية الكبرى التي تعمل في بيئات معقدة وسريعة التغير –مثل قطاع تكنولوجيا المعلومات والاتصالات– إلى تبني هيكل تنظيمي مرن يعتمد على ما يُعرف بـ "وحدات الأعمال الاستراتيجية(Strategic Business Units) " إن تقسيم المجمع إلى فروع مستقلة ليس مجرد إجراء إداري، بل هو خيار استراتيجي يهدف إلى توزيع المخاطر، وزيادة التخصص، وتسريع وتيرة اتخاذ القرار لمواكبة التطورات التكنولوجية الخاصة بكل سوق (سوق النقال، سوق الإنترنت، وسوق الاتصالات الفضائية) وسنحاول في هذا المطلب تسليط الضوء على هذه الفروع التشغيلية، متبوعة بتحليل شامل للخطط والاستراتيجيات الكلية التي تتبناها الإدارة العليا لضمان التفوق التنافسي للمجمع ككل.

أولا: فروع اتصالات الجزائر

من المنظور التسييري، يعكس إنشاء الفروع المتخصصة قدرة المؤسسة الأم على استيعاب تمايز الأسواق وتجزئتها(Market Segmentation) فإدارة شبكات الهاتف الثابت تتطلب موارد وكفاءات تختلف جذريا عن إدارة شبكات الهاتف الخلوي أو تدفق البيانات العالي. لذلك، عمدت الإدارة العليا لاتصالات الجزائر إلى هيكلة نشاطها من خلال فروع اقتصادية تتمتع بالاستقلالية والمرونة، لتتمكن من تطوير منتجاتها بشكل يتلاءم مع متطلبات كل شريحة من الزبائن، ولتساير التطورات التكنولوجية الهائلة والسريعة الحاصلة في مجال الاتصالات العالمية.

الفروع الاستراتيجية للمجمع: لقد تجسدت سياسة التنويع الاستثماري لمجمع اتصالات الجزائر في إنشاء ثلاثة فروع رئيسية وحيوية، يختص كل منها بمجال تكنولوجي محدد:

1. فرع اتصالات الجزائر "موبيليس – (Mobilis) "قطاع الهاتف الخلوي:

يُعتبر هذا الفرع بمثابة الذراع التجاري الضارب للمجمع في سوق الهاتف النقال السريع النمو، حيث يُعد أهم متعامل للهاتف الخلوي والنقال في السوق الجزائرية. من الناحية الاستثمارية والقاعدية، يرتكز فرع موبيليس على بنية تحتية قوية جدا تتجاوز 4200 محطة بث لاسلكي(BTS) ولضمان اختراق السوق

بفعالية Market Penetration، قامت الإدارة بتطوير شبكة تجارية وتسويقية واسعة تتعدى 85 وكالة تجارية خاصة بموبيليس، مدعومة بأكثر من 35,000 نقطة بيع معتمدة موزعة في أنحاء الوطن .بفضل هذه الشبكة، تمكن الفرع من تجاوز عتبة 10 ملايين مشترك، محققا نسبة تغطية جغرافية وسكانية استثنائية بلغت 98% بحلول سنة 2010 [263، 401 .]ولتعزيز تنافسيتها الدولية، ابتكرت موبيليس خدمة استراتيجية تُعرف بـ "**الاتصال المباشر الوافد Direct Inward Dialing – DID**؛ وهي خدمة أرقام افتراضية تسمح للجزائريين المغتربين في دول مثل كندا، أمريكا والبلدان الأوروبية، باقتناء رقم هاتفي جزائري، مما يتيح لعائلاتهم في الوطن الاتصال بهم بتسعيرة محلية مخفضة جدا (قُدرت بـ 4.50 دج للدقيقة)، وذلك بالشراكة الذكية مع متعاملين أجانب يتكفلون بوضع التجهيزات الضرورية هناك.

2. فرع اتصالات الجزائر للإنترنت "جواب – (Djaweb) "قطاع نقل البيانات:

في عصر اقتصاد المعرفة، أدرك المجمع أن السيطرة على تدفق البيانات هي مفتاح البقاء. لذلك، تأسس فرع "جواب" كفرع مختص حصريا في تكنولوجيا الإنترنت، حيث أُسندت إليه المهمة الاستراتيجية المتمثلة في تطوير وتوفير الإنترنت ذي السرعة الفائقة لخدمة مختلف فئات المجتمع. يعمل هذا الفرع كعصب رئيسي لربط قطاعات النشاط الكبرى في البلاد بشبكات الإنترنت، مثل التعليم العالي، البحث العلمي، التربية، التكوين المهني، الصحة، الإدارة، المحروقات، القطاع المالي، ومختلف الوزارات. من الناحية التسويقية، يعتمد الفرع على تجزئة العروض لتلائم مختلف الاحتياجات، فيقدم عروض "أنيس هوم " (Anis Home)و"أنيس إيليت (Anis Elite) " للخواص والمهنيين المستقلين بتدفقات تصل إلى 8 ميغابايت، وعروض "أنيس برو (Anis Pro) " للمؤسسات بتدفقات تصل إلى 20 ميغابايت اعتمادا على تقنيات (NGN) علاوة على ذلك، برهن هذا الفرع على كفاءة تسييرية عالية في معالجة الديون العالقة من خلال إطلاق **عرض "سهلي Sehelli"**، الذي يسمح للزبائن المقطوعة خطوطهم بجدولة ديونهم عبر أقساط مرنة، مع توفير خط تدريجي واشتراك "ويفي" عالي التدفق، بهدف استرجاع الأموال المجمدة وتقليص حظيرة الهواتف المعطلة.

3. فرع اتصالات الجزائر الفضائية – قطاع الاتصال عبر الأقمار الصناعية:

يُعد هذا الفرع مكملا حيويا للمحفظة الاستثمارية للمجمع، وهو مختص حصريا في تكنولوجيا الساتل والأقمار الصناعية. تكمن أهميته التسييرية في تقديم حلول بديلة للمؤسسات الاستراتيجية والزبائن المتواجدين في المناطق الجغرافية الوعرة التي لا تصلها الشبكات السلكية أو شبكات الهاتف النقال الكلاسيكية.

ثانيا: استراتيجيات اتصالات الجزائر

في علوم الإدارة الاستراتيجية، تُعرف "الاستراتيجية" بأنها الخطة الشاملة والمحكمة التي تحدد مسار المؤسسة وتوجه تخصيص مواردها لتحقيق الغايات طويلة الأجل وخلق ميزة تنافسية مستدامة (Sustainable Competitive Advantage). بالنسبة لمؤسسة بحجم مجمع اتصالات الجزائر، لا يمكن الاستمرار في سوق شديد الاحتدام بمجرد الاعتماد على ردود الأفعال العشوائية؛ بل يستوجب الأمر هندسة رؤية استراتيجية واضحة تتكامل فيها الأبعاد التقنية، التجارية، والتنظيمية. إن الاستراتيجية هنا هي البوصلة التي توجه استثمارات المؤسسة وتحدد كيفية تفاعلها مع الزبائن، الموردين، والمنافسين على حد سواء.

المحاور الاستراتيجية للمجمع: يعمل مجمع اتصالات الجزائر وفق مقاربة استراتيجية شمولية تهدف جميعها إلى تقديم خدمة أحسن وأجود للزبون. وترتكز هذه المقاربة على ثلاثة مستويات رئيسية متكاملة مدعومة ببرامج استثمارية ضخمة:

1. الاستراتيجية على المستوى التقني (عصرنة البنية التحتية):

تدرك الإدارة أن التفوق في عالم الاتصالات يبدأ من قوة الشبكة وحداثتها. لذا، تتبنى المؤسسة استراتيجية تقنية هجومية تعتمد على الانتشار عبر شبكة اتصالات متسلسلة حديثة، ترتكز بشكل أساسي على أحدث التكنولوجيات العالمية المتمثلة في تقنيات (IP/MPLS) وتقنيات(DWDM) الهدف التسييري من تبني هذه التكنولوجيات المكلفة هو توفير شبكة أوسع، أكثر أمانا، ومهيمنة بشكل يضمن ربطا فائق الجودة ومضمونا لكافة المتعاملين.

2. الاستراتيجية على المستوى التجاري (تعظيم القيمة وتعديل التسعير):

من الناحية التسويقية، تسعى المؤسسة للتحول من مجرد "مزود لخدمة الاتصال" إلى "مزود لحلول متكاملة". ولتحقيق ذلك، تعتمد استراتيجيتها التجارية على إطلاق منتجات وخدمات ذات قيمة مضافة عالية، إلى جانب إقامة شراكات استراتيجية (سواء على المستوى المحلي أو الدولي) للسيطرة على عدة قطاعات، لاسيما قطاع الإنترنت .كما تعتمد تكتيكا تنافسيا ذكيا يتمثل في وضع سياسة تسعيرية تهدف إلى "إعادة توازن الأسعار" عبر العروض المتطورة مثل (VAIP) وXDSL))، والعمل على تسويقها وتوزيعها بكفاءة عبر كافة نقاط شبكاتها التجارية المنتشرة في كافة ربوع الوطن.

3. الاستراتيجية على المستوى التنظيمي (الهندسة الإدارية الداخلية):

لأن التكنولوجيا المتطورة تحتاج إلى مورد بشري وتنظيم إداري فعال لاستغلالها، فقد أولت المؤسسة أهمية قصوى للبعد التنظيمي. ترتكز هذه الاستراتيجية على تحسين وتطوير وضعية الأجهزة المكلفة بخدمة الزبون، وإدارة فئة "الحسابات الكبرى Key Accounts، فضلا عن الاهتمام بالمناطق والأحياء السكنية .كما عملت الإدارة على وضع سياسة اتصال فاعلة (إعلام داخلي للموظفين وإعلام خارجي للجمهور) عبر قنوات متعددة ومدروسة. ولم تغفل عن إعداد وتصميم أدوات تسيير تقنية وتجارية حديثة للرفع من مستوى الرقابة وتحسين أداء التنظيم الداخلي.

4. المشاريع الاستثمارية الداعمة للاستراتيجيات: (CAPEX)

في علوم التسيير المالي، تترجم الاستراتيجيات دائما إلى نفقات استثمارية (Capital Expenditures) وفي إطار سعيها الحثيث لتحسين خدماتها وتجسيد استراتيجياتها التقنية والتجارية، قام مجمع اتصالات الجزائر بضخ أموال ضخمة في حزمة من الاستثمارات الهيكلية الكبرى، لعل من أبرزها

- مشروع إنجاز شبكة واسعة ومتعددة الخدمات تتميز بقدرات ربط هائلة سلسلة IMMPLS التي توفر شبكات مزودة بعدة خدمات ومراقبة إجمالية.
- المشروع الاستراتيجي للكابل البحري للألياف البصرية (SEA NE WE4) الذي يضمن ربط الجزائر بقارة أوروبا عبر وصلات عالية السعة والسرعة.
- مشروع نشر تقنية الهاتف الثابت دون خط عبر تكنولوجيا (CDMA–EVDO/WL) لتوسيع الكثافة الهاتفية في الأماكن التي يصعب ربطها سلكيا.
- مشاريع التوسعة المستمرة لشبكات اتصالات الجزائر الخاصة بالإنترنت لتغطية الطلب المتزايد.
- مشروع توسيع شبكة اتصالات الجزائر عبر الأقمار الصناعية لضمان تغطية جغرافية شاملة.
- مشاريع التقنيات اللاسلكية ذات النطاق العريض مثل مشاريع WIMA– WIFI

المطلب الثالث: الهيكل التنظيمي لمؤسسة اتصالات الجزائر (نموذج المديرية العملية)

الهيكل التنظيمي (Organizational Structure) هو الهيكل العظمي لأي مؤسسة، وهو الذي يوضح قنوات الاتصال، تسلسل السلطة، ونطاق الإشراف، بالإضافة إلى كيفية توزيع المهام بين الأقسام. ونظرا لاتساع حجم مجمع اتصالات الجزائر، فقد اتبع سياسة اللامركزية في التسيير(Decentralization) لتقريب الإدارة من المواطن. يتجلى ذلك من خلال الهياكل التنظيمية للوحدات والمديريات العملية (مثل وحدة تبسة أو وحدة ورقلة)، التي تعتبر المستوى الثالث بعد المديرية الإقليمية، حيث مُنحت سلطات واسعة في التسيير والإشراف للرفع من الكفاءة الإنتاجية والاستجابة السريعة لمشاكل الزبائن.

الهيكل التنظيمي للمديرية العملية: تنقسم المديرية العملية التابعة لمؤسسة اتصالات الجزائر إلى هياكل إدارية متكاملة تتكون أساسا من "خلايا" متخصصة و"دوائر" إدارية تضم تحتها مجموعة من المصالح والمكاتب.

أ. **الخلايا المتخصصة:(Staff/Support Cells)** تمثل الأجهزة الاستشارية والرقابية التابعة مباشرة لمدير المديرية العملية، وتشمل:

- **الخلية التفتيشية:** تسهر على تطبيق القوانين وفتح التحقيقات الميدانية (مثل التعدي على الكوابل وسرقتها)
- **خلية العلاقات الخارجية:** تهدف إلى تحسين وتلميع الصورة الذهنية للمؤسسة أمام الزبائن والمستثمرين، وتمثيل المؤسسة رسميا .
- **خلية الأمن الداخلي:** تعمل على توفير الوسائل اللازمة لحماية مقرات الإدارة، وتعيين فرق الحراسة لضمان أمن الممتلكات.
- **الخلية النوعية (الجودة):** تضطلع بمهام متابعة ومراقبة مخطط عمل المؤسسة، والتأكد من السعي السليم لتحقيق الأهداف المسطرة.

ب. **الدوائر الوظيفية:(Functional Departments)** وهي التقسيمات الأساسية التي تتولى تنفيذ المهام التسييرية والتشغيلية الكبرى، وتضم أربع دوائر رئيسية.

- **دائرة المالية والمحاسبة والشؤون القانونية:** تهتم بالجانب المالي وتسديد الفواتير والضرائب. وتضم "مصلحة المحاسبة" التي تسجل العمليات المحاسبية اليومية وتتابع مستحقات الزبائن، و"مصلحة الميزانية" لضبط النفقات وإعداد وضعية إقفال الحسابات. بالإضافة إلى "مصلحة

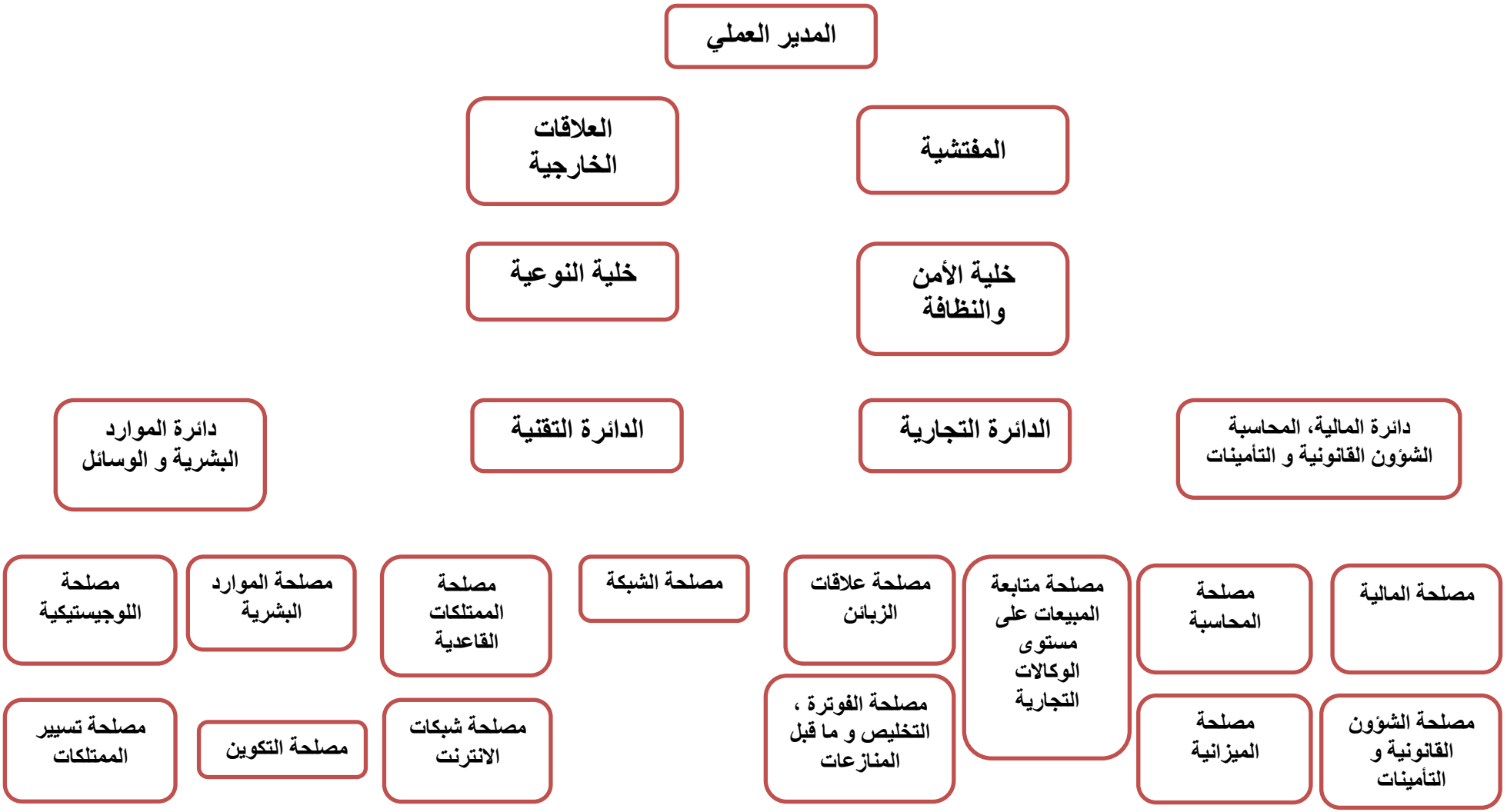
الشؤون القانونية والتأمينات" لحماية ممتلكات المؤسسة قانونيا ورفع الشكاوى لمصالح الأمن ضد التعديات .

- **دائرة الموارد البشرية والوسائل (اللوجستية):** من أهم الدوائر الإدارية، تتفرع إلى "مصلحة الموارد البشرية" التي تدير الحياة المهنية للعمال، التوظيف، الأجور، الترقية، وتكاليف التكوين. وتضم "مصلحة تسيير الممتلكات" المكلفة بإدارة وتسيير المخازن وإحصاء الممتلكات. كما تضم "المصلحة اللوجستية" (مكاتب النقل، البناء، والإمداد) لضمان توفير وتأمين كافة الاحتياجات المادية، التجهيزات، وأدوات العمل للمكاتب الإدارية والتقنية.

- **الدائرة التقنية:** هي العصب التشغيلي للمديرية، وتشمل "مصلحة الشبكة" المعنية بتركيب الخطوط ومراقبة الإنتاج، و"مصلحة الممتلكات القاعدية" التي تعد الدراسات والمخططات لصيانة وبناء المراكز الهاتفية وإدارة عمليات الإرسال والاستبدال، فضلا عن "مصلحة شبكات الإنترنت" المخصصة لمتابعة وصيانة تكنولوجيا تدفق البيانات.

- **الدائرة التجارية:** وتمثل واجهة المؤسسة أمام الجمهور. تتضمن "مصلحة علاقات الزبائن" لمعالجة الشكاوى والاستفسارات، و"مصلحة الفوترة وما قبل المنازعات" المكلفة بإعداد الفواتير ومتابعة الزبائن المدينين وتحويل ملفاتهم عند الضرورة للمنازعات، إضافة إلى "مصلحة متابعة المبيعات" التي تعد الإحصائيات الدورية (أسبوعية، شهرية، وسنوية) لتقييم الأداء التجاري للوكالات.

الشكل رقم (1): الهيكل التنظيمي لمؤسسة اتصالات الجزائر وحدة تبسة



المبحث الثاني: إجراءات الدراسة الميدانية

يهدف هذا المبحث إلى عرض الإجراءات المنهجية المعتمدة في الدراسة الميدانية، من خلال تحديد أداة جمع البيانات، ومجتمع وعينة الدراسة، وخصائص الاستبيان، إضافة إلى اختبار صدق وثبات الأداة وتحليل النتائج الوصفية واختبار الفرضيات.

وقد تم الاعتماد على استبيان افتراضي موجه إلى كل من موظفي وعملاء الوكالة التجارية لاتصالات الجزائر، بهدف قياس فعالية الأمن السيبراني في حماية بيانات العملاء، مع مراعاة توحيد العبارات حتى تكون مناسبة للفئتين معا.

المطلب الأول: منهجية الدراسة الميدانية

أولا: أداة الدراسة

تم الاعتماد في هذه الدراسة على الاستبيان كأداة رئيسية لجمع البيانات، باعتباره من أكثر الأدوات استخداما في الدراسات الميدانية التي تهدف إلى قياس اتجاهات وآراء الأفراد حول موضوع معين.

وقد تم تصميم الاستبيان بما يتناسب مع موضوع الدراسة، حيث وجه الاستبيان إلى فئتين أساسيتين هما:

موظفو الوكالة التجارية لاتصالات الجزائر .

عملاء الوكالة التجارية لاتصالات الجزائر .

والجدول التالي صممناه خصيصا لوصف أداة الدراسة:

جدول رقم (01): هيكلة الاستبيان

القسم	المحور / البعد	مضمون المحور	عدد الفقرات	أرقام الفقرات
القسم الأول	البيانات الشخصية والديمغرافية	يتضمن خصائص أفراد العينة من حيث الجنس، الفئة العمرية، المستوى التعليمي، وصفة المستجيب: موظف أو عميل.	4	من 1 إلى 4
القسم الثاني	المحور الأول: تقييم الآليات التقنية	يقيس مدى توفر الإجراءات التقنية والتنظيمية التي تعتمدها المؤسسة لحماية خدماتها الرقمية،	8	من 1 إلى 8

	والتنظيمية للأمن السيبراني	مثل أنظمة التحقق، تحديث المنصات، الإشعارات الأمنية، والتعامل مع البلاغات الرقمية.		
القسم الثاني	المحور الثاني: فعالية حماية خصوصية وسرية البيانات	يقيس مدى احترام المؤسسة لخصوصية البيانات الشخصية وسرية المعاملات الإلكترونية، وحماية المعلومات من الوصول غير المصرح به، وتوضيح سياسة حماية البيانات.	8	من 9 إلى 16
القسم الثاني	المحور الثالث: الانعكاسات التسويقية للأمن السيبراني	يقيس أثر الأمن السيبراني في تعزيز الثقة في المؤسسة، وتحسين صورتها في السوق، وزيادة الرغبة في الاستمرار في التعامل معها والتوصية بخدماتها.	8	من 17 إلى 24
—	مجموع فقرات الاستبيان	يشمل جميع الفقرات الخاصة بمحاور الدراسة دون احتساب البيانات الشخصية والديمغرافية.	24	من 1 إلى 24

تم تقسيم الاستبيان إلى قسمين رئيسيين؛ حيث خصص القسم الأول للبيانات الشخصية والديمغرافية لأفراد العينة، بهدف التعرف على خصائصهم العامة، بينما خصص القسم الثاني لمحاور الدراسة المرتبطة بموضوع فعالية الأمن السيبراني في حماية بيانات العملاء. وقد تضمن هذا القسم ثلاثة محاور أساسية، بواقع ثماني فقرات لكل محور، أي ما مجموعه أربع وعشرون فقرة. ويعكس هذا التقسيم توازنا في بناء أداة الدراسة، إذ يسمح بقياس الجوانب التقنية والتنظيمية للأمن السيبراني، ومدى فعاليته في حماية خصوصية وسرية البيانات، إضافة إلى آثاره التسويقية على ثقة العملاء وصورة المؤسسة.

ثانيا: مجتمع وعينة الدراسة

يتكون مجتمع الدراسة من موظفي وعملاء الوكالة التجارية لاتصالات الجزائر محل الدراسة، ونظرا لصعوبة دراسة المجتمع ككل، تم الاعتماد على عينة قصدية مكونة من موظفين وعملاء لهم علاقة مباشرة بالخدمات الرقمية للمؤسسة.

وقد تم توزيع 40 استمارة، منها:

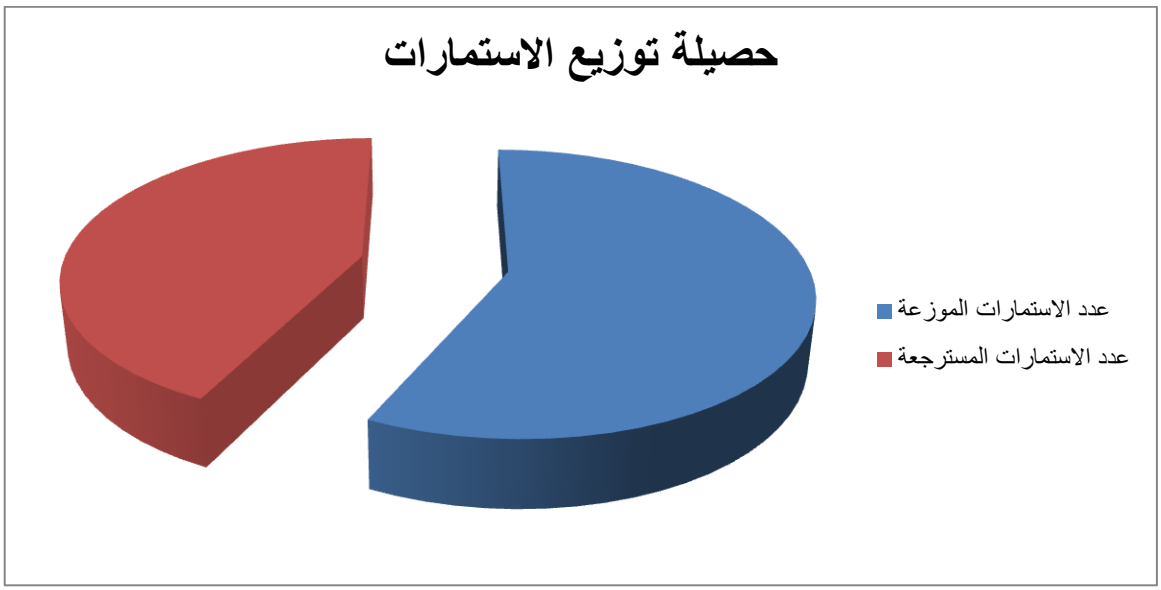
20 استمارة على الموظفين

20 استمارة على العملاء

وتم استرجاع 30 استمارة صالحة للتحليل، موزعة كما في الجدول التالي:

جدول رقم (02): حصيلة توزيع الاستمارات

الفئة	عدد الاستمارات الموزعة	عدد الاستمارات المسترجعة	نسبة الاسترجاع
الموظفون	20	15	75%
العملاء	20	15	75%
المجموع	40	30	75%



الشكل رقم (02): يوضح حصيلة توزيع الاستمارات

يتضح لنا من الجدول أن عدد الاستمارات المسترجعة بلغ 30 استمارة من أصل 40 استمارة موزعة، أي بنسبة استرجاع قدرها 75%، وهي نسبة مقبولة في الدراسات الميدانية، خاصة أن العينة تضم فئتين مختلفتين هما الموظفون والعملاء، مما يسمح بالحصول على رؤية أكثر شمولا حول فعالية الأمن السيبراني في حماية بيانات العملاء.

ثالثا: خصائص الاستبيان

تم تصميم الاستبيان بشكل منظم، حيث تضمن قسما خاصا بالبيانات الشخصية والديمغرافية، وقسما آخر خاصا بمحاور الدراسة، والتي بلغت ثلاثة محاور رئيسية بإجمالي 24 فقرة، كما تم الاعتماد على مقياس ليكرت الخماسي لقياس اتجاهات أفراد العينة، وهو من المقاييس المناسبة للدراسات السلوكية والإدارية والتسويقية، نظرا لقدرته على قياس درجة الموافقة أو عدم الموافقة على العبارات المطروحة، يوضح الجدول الآتي الخصائص العامة للاستبيان المعتمد في الدراسة[1]:

جدول رقم (03): خصائص الاستبيان

الخاصية	التوضيح
المؤسسة محل الدراسة	الوكالة التجارية لاتصالات الجزائر
الفئة المستهدفة	الموظفون والعملاء
عدد الاستمارات الموزعة	40استمارة
عدد الاستمارات المسترجعة والصالحة للتحليل	30استمارة
طبيعة الدراسة	دراسة ميدانية وصفية تحليلية
أداة جمع البيانات	الاستبيان
عدد أقسام الاستبيان	قسمان رئيسيان
القسم الأول	البيانات الشخصية والديمغرافية
القسم الثاني	محاور الدراسة
عدد محاور الدراسة	3محاور
عدد فقرات المحور الأول	8فقرات
عدد فقرات المحور الثاني	8فقرات

[1] – ينظر الملحق رقم 1 من أجل لاستبيان المستخدم في الدراسة الميدانية.

عدد فقرات المحور الثالث	8 فقرات
إجمالي فقرات الاستبيان دون البيانات الشخصية	24 فقرة
مقياس القياس	مقياس ليكرت الخماسي

3-1- مقياس الاستبيان

تم استخدام مقياس ليكرت الخماسي لقياس إجابات أفراد العينة، ولتفسير المتوسطات الحسابية، تم اعتماد المجالات كما هو موضح في الجدول الآتي:

جدول رقم (04): مقياس الاستبيان

درجة الموافقة	الرمز العددي	المجال	مستوى الموافقة
غير موافق بشدة	1	من 1.00 إلى 1.80	منخفض جدا
غير موافق	2	من 1.81 إلى 2.60	منخفض
محايد	3	من 2.61 إلى 3.40	متوسط
موافق	4	من 3.41 إلى 4.20	مرتفع
موافق بشدة	5	من 4.21 إلى 5.00	مرتفع جدا

يسمح لنا مقياس ليكرت الخماسي بقياس اتجاهات أفراد العينة بدرجة مناسبة من الدقة، حيث يتيح التمييز بين مستويات مختلفة من الموافقة، بدءا من عدم الموافقة الشديدة وصولا إلى الموافقة الشديدة. كما يساعد هذا المقياس في استخراج المتوسطات الحسابية والانحرافات المعيارية، مما يسمح بتحليل اتجاهات العينة نحو محاور الدراسة.

رابعا: اختبار صدق وثبات أداة الدراسة

4-1- ثبات أداة الدراسة

تم الاعتماد على معامل ألفا كرونباخ لقياس ثبات أداة الدراسة، أي مدى اتساق فقرات كل محور في قياس البعد الذي تنتمي إليه. وكلما اقتربت قيمة ألفا كرونباخ من الواحد الصحيح، دل ذلك على ارتفاع درجة الثبات، والجدول الآتي يوضح النتائج الافتراضية لاختبار الثبات:

جدول رقم (05): ثبات أداة الدراسة

المحاور	عدد الفقرات	معامل ألفا كرونباخ
المحور الأول: الآليات التقنية والتنظيمية للأمن السيبراني	8	0.842
المحور الثاني: حماية خصوصية وسرية البيانات	8	0.876
المحور الثالث: الانعكاسات التسويقية للأمن السيبراني	8	0.861
الاستبيان ككل دون البيانات الشخصية	24	0.924

المصدر: من إعداد الطالب بالاعتماد على بيانات افتراضية محاكية لمخرجات SPSS v27.

قيم معامل ألفا كرونباخ المسجلة تراوحت بين 0.842 و0.876 بالنسبة لمحاور الدراسة، وهي قيم مرتفعة تدل على وجود اتساق داخلي جيد بين فقرات كل محور، كما بلغت قيمة معامل الثبات للاستبيان ككل 0.924، وهي قيمة مرتفعة جدا، مما يشير إلى أن أداة الدراسة تتمتع بدرجة عالية من الثبات، ويمكن الاعتماد عليها في تحليل نتائج الدراسة واختبار فرضياتها.

4-2- صدق أداة الدراسة

أ- الصدق الظاهري

تم التأكد من الصدق الظاهري للاستبيان من خلال عرضه في صورته الأولية على مجموعة من الأساتذة والمتخصصين في مجال الإدارة والتسويق ونظم المعلومات، بهدف التأكد من مدى وضوح العبارات، وسلامة صياغتها، ومدى ارتباطها بمحاور الدراسة، وقد تم الأخذ بالملاحظات المقترحة، خاصة ما تعلق بتوحيد صياغة العبارات لتناسب كلا من الموظفين والعملاء، وتصحيح بعض المصطلحات، وتبسيط العبارات المرتبطة بحماية البيانات والأمن السيبراني، بناء على ذلك، يمكن القول إن الاستبيان يتمتع بدرجة مقبولة من الصدق الظاهري.

ب- الاتساق الداخلي لعبارات المحاور

تم اختبار الصدق البنائي من خلال قياس العلاقة بين كل محور والدرجة الكلية للاستبيان، وذلك باستعمال معامل ارتباط بيرسون.

جدول رقم (06): الاتساق الداخلي لعبارات المحاور

المحاور	معامل الارتباط مع الدرجة الكلية	مستوى الدلالة
المحور الأول: الآليات التقنية والتنظيمية للأمن السيبراني	0.781	0.000
المحور الثاني: حماية خصوصية وسرية البيانات	0.826	0.000
المحور الثالث: الانعكاسات التسويقية للأمن السيبراني	0.798	0.000

المصدر: من إعداد الطالب بالاعتماد على بيانات افتراضية محاكية لمخرجات SPSS v27.

تشير النتائج إلى وجود علاقات ارتباط موجبة وقوية بين كل محور من محاور الدراسة والدرجة الكلية للاستبيان، حيث تراوحت معاملات الارتباط بين 0.781 و0.826، وهي قيم دالة إحصائيا عند مستوى معنوية 0.05، نظرا لأن قيمة الدلالة الإحصائية بلغت 0.000، وهي أقل من 0.05. وهذا يدل على أن محاور الاستبيان تتمتع بدرجة جيدة من الصدق البنائي، وأنها تقيس فعليا الأبعاد المرتبطة بموضوع الدراسة.

خامسا: اختبار التوزيع الطبيعي للبيانات

قبل اختبار الفرضيات، نجد من الضرورة المنهجية الاعتماد على اختبار كولموغروف-سيميرنوف للتحقق من مدى خضوع البيانات للتوزيع الطبيعي، وذلك لتحديد مدى ملاءمة استخدام الاختبارات المعلمية، مثل معامل ارتباط بيرسون.

جدول رقم (07): اختبار التوزيع الطبيعي للبيانات

المحاور	قيمة كولموغروف–سيميرنوف	درجة الحرية	مستوى الدلالة
المحور الأول: الآليات التقنية والتنظيمية للأمن السيبراني	0.113	30	0.200
المحور الثاني: حماية خصوصية وسرية البيانات	0.126	30	0.184
المحور الثالث: الانعكاسات التسويقية للأمن السيبراني	0.119	30	0.200
الدرجة الكلية للاستبيان	0.108	30	0.200

المصدر: من إعداد الطالب بالاعتماد على بيانات افتراضية محاكية لمخرجات SPSS v27.

من الجدول أعلاه، يتبين أنّ مستوى الدلالة لجميع محاور الدراسة أكبر من 0.05، مما يدل على أن البيانات تتبع التوزيع الطبيعي. وبناء على ذلك، يمكن استخدام الاختبارات الإحصائية المعلمية، وعلى رأسها معامل ارتباط بيرسون، لاختبار فرضيات الدراسة فيما بعد.

المطلب الثاني: التحليل الوصفي لبيانات الاستبيان

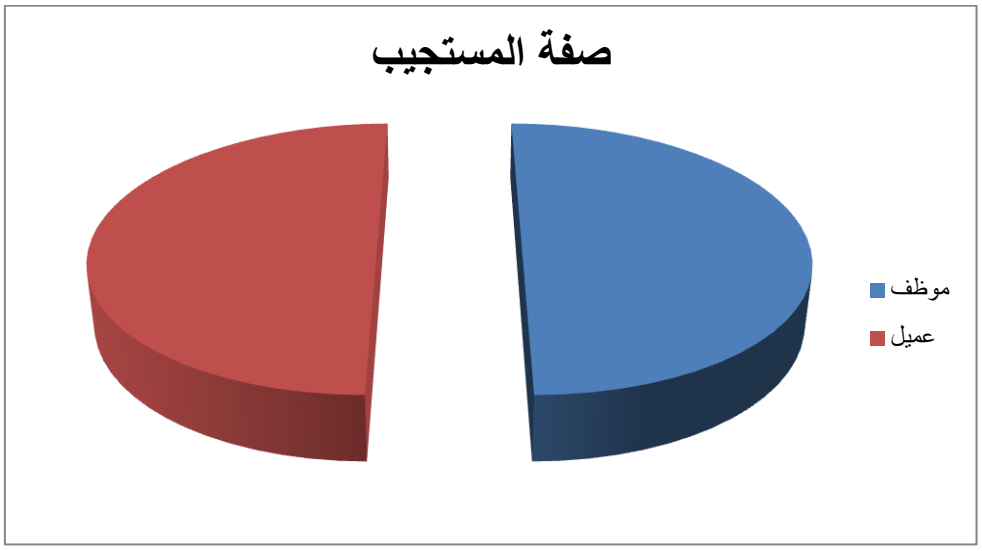
أولا: تحليل البيانات الشخصية والديمغرافية

1- توزيع أفراد العينة حسب صفة المستجيب

جدول رقم (08): توزيع أفراد العينة حسب صفة المستجيب

صفة المستجيب	التكرار	النسبة المئوية
موظف	15	50%
عميل	15	50%
المجموع	30	100%

المصدر :من إعداد الطالب بالاعتماد على بيانات الاستبيان



الشكل رقم (03): يوضح توزيع أفراد العينة حسب صفة المستجيب

يتضح من الجدول أن أفراد عينة الدراسة توزعوا بالتساوي بين فئتي الموظفين والعملاء، حيث مثلت كل فئة نسبة 50% من إجمالي العينة. ويعكس هذا التوزيع توازنا في تمثيل الفئتين محل الدراسة، مما يسمح بالحصول على رؤية أكثر شمولا حول موضوع فعالية الأمن السيبراني في حماية بيانات العملاء.

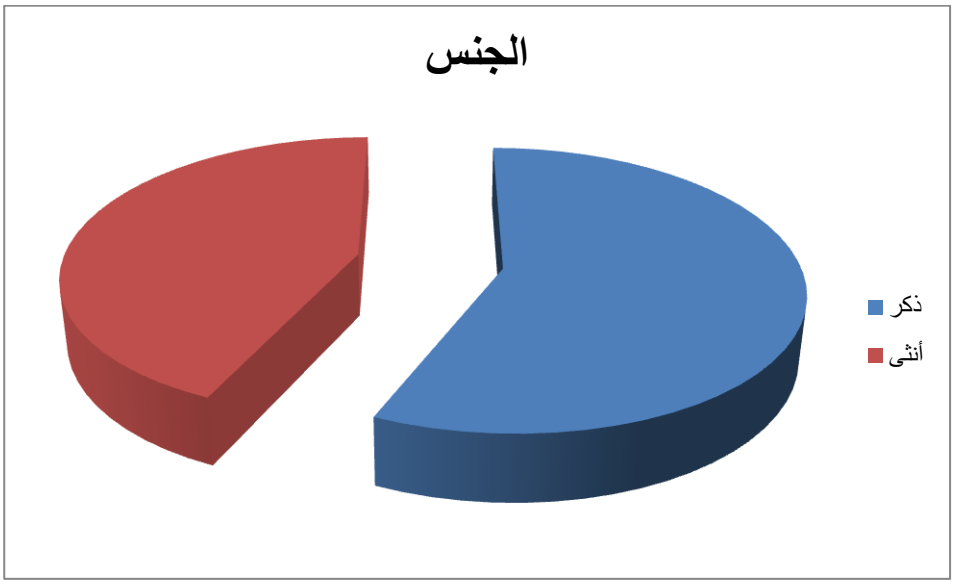
فالموظفون يعكسون وجهة النظر الداخلية المرتبطة بالإجراءات والسياسات الأمنية المعتمدة داخل المؤسسة، في حين يعكس العملاء وجهة النظر الخارجية المرتبطة بمستوى الثقة والإحساس بالأمان عند استخدام الخدمات الرقمية للمؤسسة.

2- توزيع أفراد العينة حسب الجنس

جدول رقم (09): توزيع أفراد العينة حسب الجنس

الجنس	التكرار	النسبة المئوية
ذكر	17	56.7%
أنثى	13	43.3%
المجموع	30	100%

المصدر :من إعداد الطالب بالاعتماد على بيانات الاستبيان



الشكل رقم (04): توزيع أفراد العينة حسب الجنس

فئة الذكور تمثل النسبة الأكبر من أفراد العينة بنسبة 56.7%، في حين تمثل فئة الإناث نسبة 43.3%. ويشير هذا التوزيع إلى وجود تقارب نسبي بين الجنسين، مع تفوق طفيف لفئة الذكور.

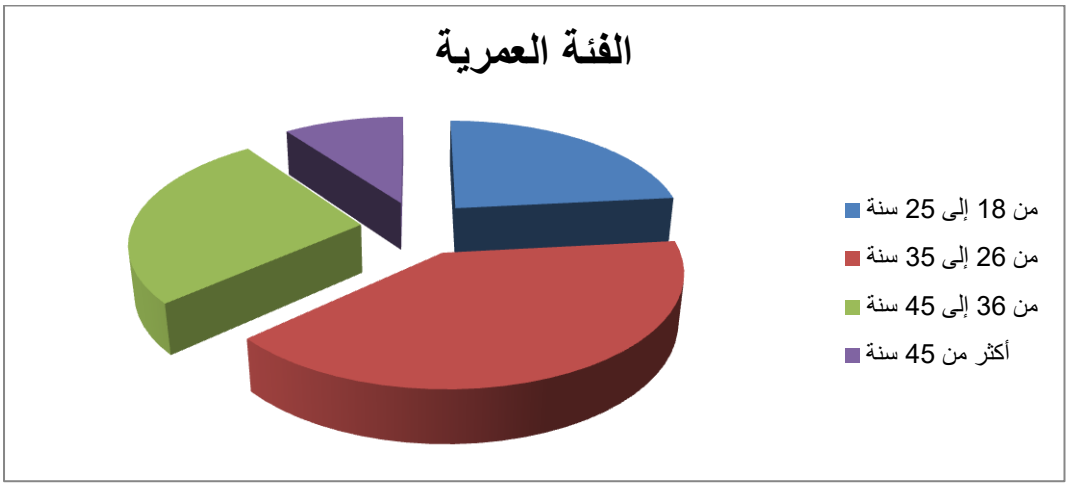
كما يعكس هذا التنوع في العينة إمكانية الحصول على آراء مختلفة حول موضوع فعالية الأمن السيبراني في حماية بيانات العملاء، باعتبار أن استخدام الخدمات الرقمية والتعامل مع البيانات الإلكترونية لا يقتصر على فئة معينة دون أخرى.

3- توزيع أفراد العينة حسب الفئة العمرية

جدول رقم (10): توزيع أفراد العينة حسب الفئة العمرية

الفئة العمرية	التكرار	النسبة المئوية
من 18 إلى 25 سنة	7	23.3%
من 26 إلى 35 سنة	12	40%
من 36 إلى 45 سنة	8	26.7%
أكثر من 45 سنة	3	10%
المجموع	30	100%

المصدر :من إعداد الطالب بالاعتماد على بيانات الاستبيان



الشكل رقم (05): توزيع أفراد العينة حسب الفئة العمرية

الفئة العمرية من 26 إلى 35 سنة تمثل النسبة الأكبر من أفراد العينة بنسبة 40%، تليها فئة 36إلى 45 سنة بنسبة 26.7%، ثم فئة 18إلى 25 سنة بنسبة 23.3%، في حين جاءت فئة أكثر من 45 سنة في المرتبة الأخيرة بنسبة .10%

ويشير هذا التوزيع إلى أن أغلب أفراد العينة ينتمون إلى فئات عمرية نشطة، وهو ما قد يعزز قدرتهم على التعامل مع الخدمات الرقمية للمؤسسة وإبداء آرائهم حول مستوى الأمن السيبراني وحماية البيانات الشخصية.

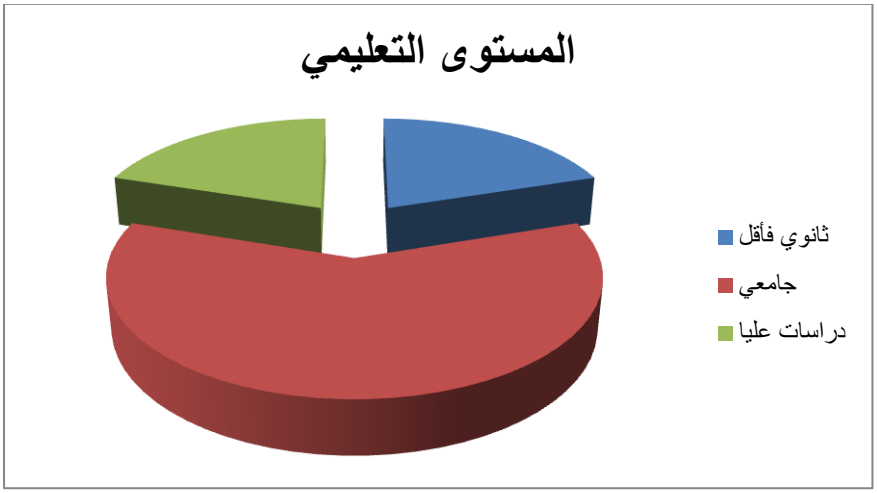
يتضح أن الفئة العمرية الأكثر تمثيلا هي فئة من 26 إلى 35 سنة بنسبة 40%، تليها فئة من 36 إلى 45 سنة بنسبة 26.7%. وهذا يشير إلى أن أغلب أفراد العينة ينتمون إلى فئات عمرية نشطة ولديها تعامل معتبر مع الخدمات الرقمية.

4- توزيع أفراد العينة حسب المستوى التعليمي

جدول رقم (11): توزيع أفراد العينة حسب المستوى التعليمي

المستوى التعليمي	التكرار	النسبة المئوية
ثانوي فأقل	6	20%
جامعي	18	60%
دراسات عليا	6	20%
المجموع	30	100%

المصدر :من إعداد الطالب بالاعتماد على بيانات الاستبيان



الشكل رقم (06): توزيع أفراد العينة حسب المستوى التعليمي

فئة المستوى الجامعي تمثل النسبة الأكبر من أفراد العينة بنسبة 60%، في حين جاءت فئتا ثانوي فأقل ودراسات عليا بنسبة متساوية بلغت 20%لكل منهما.

ويشير هذا التوزيع إلى أن أغلب أفراد العينة يتمتعون بمستوى تعليمي يسمح لهم بفهم طبيعة الأسئلة المطروحة في الاستبيان، خاصة أن موضوع الدراسة يرتبط بالأمن السيبراني وحماية البيانات الشخصية، وهي مواضيع تتطلب قدرا معينا من الوعي بالخدمات الرقمية والتعاملات الإلكترونية.

الخصائص العامة للعينة ملائمة لطبيعة الدراسة، حيث تجمع بين التنوع في الجنس والعمر، والتوازن بين الموظفين والعملاء، إضافة إلى مستوى تعليمي مناسب، مما يدعم إمكانية الاعتماد على آرائهم في تحليل فعالية الأمن السيبراني في حماية بيانات العملاء داخل المؤسسة محل الدراسة.

ثانيا: تحليل محاور الدراسة

بهدف التعرف على اتجاهات المستجيبين نحو العبارات المرتبطة بموضوع فعالية الأمن السيبراني في حماية بيانات العملاء تم الاعتماد على المتوسطات الحسابية والانحرافات المعيارية، من أجل تحديد درجة موافقة أفراد العينة على فقرات كل محور من محاور الاستبيان، كما تم تفسير النتائج بالاستناد إلى مقياس ليكرت الخماسي سابق الذكر، الذي يوضح مستوى الموافقة من منخفض جدا إلى مرتفع جدا، والنتائج كالتالي.

1- نتائج المحور الأول: تقييم الآليات التقنية والتنظيمية للأمن السيبراني

جدول رقم (12): يوضح نتائج المحور 1 (تقييم الآليات التقنية والتنظيمية للأمن السيبراني)

رقم الفقرة	المتوسط الحسابي	الانحراف المعياري	مستوى الموافقة
1	3.93	0.81	مرتفع
2	4.10	0.76	مرتفع
3	3.62	0.88	مرتفع
4	3.87	0.79	مرتفع
5	3.55	0.91	مرتفع
6	3.71	0.84	مرتفع
7	3.68	0.86	مرتفع
8	3.74	0.82	مرتفع
المتوسط العام للمحور	3.78	0.83	مرتفع

المصدر :من إعداد الطالب بالاعتماد على بيانات الاستبيان

- أيضا قيمة المتوسط الحسابي للفقرة الأولى 3.93، بانحراف معياري قدره 0.81، وهو ما يقابل مستوى موافقة مرتفع .ويدل ذلك على أن أفراد العينة يرون أن المؤسسة توفر بيئة رقمية آمنة نسبيا عند استخدام خدماتها الإلكترونية، مما يعكس وجود اهتمام واضح بتوفير الحماية الأساسية للمستخدمين.

- بلغ المتوسط الحسابي للفقرة الثانية 4.10، بانحراف معياري قدره 0.76، وهو مستوى موافقة مرتفع .وتعد هذه الفقرة الأعلى ضمن المحور، مما يشير إلى أن أفراد العينة يلاحظون اعتماد المؤسسة على أنظمة تحقق فعالة، مثل كلمات المرور ورموز التحقق والمصادقة المزدوجة، بهدف تعزيز أمن الحسابات الرقمية.

– قيمة المتوسط الحسابي للفقرة الثالثة 3.62، بانحراف معياري قدره 0.88، وهو مستوى موافقة مرتفع .ويعكس ذلك أن المؤسسة تقوم إلى حد معتبر بإشعار المستخدمين بأي نشاط غير عادي يتعلق بحساباتهم أو معاملاتهم، غير أن المتوسط الأقل نسبيا مقارنة ببعض الفقرات الأخرى يدل على إمكانية تحسين آليات التنبيه والإشعار الأمني.

– والمتوسط الحسابي للفقرة الرابعة 3.87، بانحراف معياري قدره 0.79، وهو مستوى موافقة مرتفع .ويشير ذلك إلى أن أفراد العينة يرون أن المؤسسة تقوم بتحديث منصاتها الرقمية بانتظام من أجل تعزيز مستوى الأمان، وهو ما يعد مؤشرا إيجابيا على متابعة المؤسسة للتطورات التقنية والمخاطر الرقمية.

– كذلك المتوسط الحسابي للفقرة الخامسة 3.55، بانحراف معياري قدره 0.91، وهو مستوى موافقة مرتفع .ورغم أن النتيجة إيجابية، إلا أن هذه الفقرة سجلت أدنى متوسط داخل المحور، مما يشير إلى أن التعليمات والإرشادات المتعلقة بالاستخدام الآمن للخدمات الرقمية تحتاج إلى مزيد من التوضيح والتعزيز، سواء بالنسبة للعملاء أو الموظفين.

– بلغ المتوسط الحسابي للفقرة السادسة 3.71، بانحراف معياري قدره 0.84، وهو مستوى موافقة مرتفع .ويعني ذلك أن أفراد العينة يرون أن المؤسسة تتعامل بجدية مع البلاغات المتعلقة بالمشكلات أو المخاطر الرقمية، مما يعكس وجود وعي تنظيمي بأهمية الاستجابة السريعة للمخاطر السيبرانية.

– بلغ المتوسط الحسابي للفقرة السابعة 3.68، بانحراف معياري قدره 0.86، وهو مستوى موافقة مرتفع .ويدل ذلك على أن المؤسسة تعتمد إجراءات للحد من محاولات الاختراق أو الاحتيال عبر منصاتها الرقمية، إلا أن المتوسط يشير أيضا إلى إمكانية تطوير هذه الإجراءات وتعزيز ثقة المستخدمين في فعاليتها.

– المتوسط الحسابي للفقرة الثامنة 3.74، بانحراف معياري قدره 0.82، وهو مستوى موافقة مرتفع .ويشير ذلك إلى أن أفراد العينة يدركون وجود إجراءات تنظيمية واضحة تحكم استخدام الخدمات الإلكترونية داخل المؤسسة، مما يساهم في تنظيم التعاملات الرقمية وتقليل المخاطر المرتبطة بسوء الاستخدام.

النتيجة العامة للمحور الأول

عموما، بلغت قيمة المتوسط الحسابي العام للمحور الأول 3.78، بانحراف معياري قدره 0.83، وهو مستوى موافقة مرتفع .وبناء على ذلك، يمكن القول إن أفراد العينة لديهم تقييم إيجابي للآليات التقنية والتنظيمية للأمن السيبراني داخل المؤسسة، خاصة فيما يتعلق بأنظمة التحقق وتحديث المنصات الرقمية. ومع ذلك، تشير النتائج إلى وجود بعض الجوانب التي يمكن تحسينها، خصوصا ما يتعلق بتوضيح تعليمات الاستخدام الآمن وتعزيز آليات الإشعار والتنبيه بالمخاطر الرقمية.

نتائج المحور الثاني: فعالية حماية خصوصية وسرية البيانات

جدول رقم (13): يوضح نتائج المحور 2 (فعالية حماية خصوصية وسرية البيانات)

رقم الفقرة	المتوسط الحسابي	الانحراف المعياري	مستوى الموافقة
1	4.02	0.74	مرتفع
2	3.96	0.79	مرتفع
3	3.88	0.81	مرتفع
4	3.72	0.87	مرتفع
5	3.81	0.85	مرتفع
6	3.59	0.90	مرتفع
7	3.91	0.78	مرتفع
8	4.05	0.73	مرتفع
المتوسط العام للمحور	3.87	0.81	مرتفع

المصدر :من إعداد الطالب بالاعتماد على بيانات الاستبيان

– المتوسط الحسابي للفقرة الأولى 4.02، بانحراف معياري قدره 0.74، وهو ما يقابل مستوى موافقة مرتفع .ويدل ذلك على أن أفراد العينة يرون أن المؤسسة تحترم خصوصية البيانات الشخصية عند استخدام الخدمات الرقمية، مما يعكس وجود إدراك إيجابي لمستوى التزام المؤسسة بحماية خصوصية المستخدمين.

الفقرة الثانية

– المتوسط الحسابي للفقرة الثانية 3.96، بانحراف معياري قدره 0.79، وهو مستوى موافقة مرتفع .ويشير ذلك إلى أن المؤسسة تطلب، حسب رأي أفراد العينة، البيانات الضرورية فقط لإتمام المعاملات، وهو ما يعكس توجها إيجابيا نحو تقليل جمع البيانات غير الضرورية.

الفقرة الثالثة

– أيضا المتوسط الحسابي للفقرة الثالثة 3.88، بانحراف معياري قدره 0.81، وهو مستوى موافقة مرتفع .ويدل ذلك على أن أفراد العينة يعتقدون أن المؤسسة تعمل على حماية المعلومات الشخصية من الوصول غير المصرح به، مما يعزز الثقة في الإجراءات الأمنية المعتمدة.

– قيمة المتوسط الحسابي للفقرة الرابعة 3.72، بانحراف معياري قدره 0.87، وهو مستوى موافقة مرتفع .ويعكس ذلك شعورا إيجابيا نسبيا بالأمان عند إدخال المعلومات الحساسة، مثل بيانات الهوية أو الدفع، إلا أن المتوسط الأقل مقارنة ببعض الفقرات الأخرى يشير إلى إمكانية تعزيز مستوى الطمأنينة لدى المستخدمين.

– بلغ المتوسط الحسابي للفقرة الخامسة 3.81، بانحراف معياري قدره 0.85، وهو مستوى موافقة مرتفع .ويشير ذلك إلى أن أفراد العينة يميلون إلى الاعتقاد بأن المؤسسة لا تشارك البيانات الشخصية مع أطراف أخرى دون موافقة صاحبها، مما يعكس أهمية الالتزام بمبدأ سرية البيانات.

– المتوسط الحسابي للفقرة السادسة 3.59، بانحراف معياري قدره 0.90، وهو مستوى موافقة مرتفع .ورغم أن النتيجة إيجابية، إلا أن هذه الفقرة سجلت أدنى متوسط داخل المحور، مما يدل على أن سياسة حماية البيانات قد تحتاج إلى توضيح أكبر للمستخدمين، سواء من حيث طريقة عرضها أو سهولة فهمها.

كذلك قيمة المتوسط الحسابي للفقرة السابعة 3.91، بانحراف معياري قدره 0.78، وهو مستوى موافقة مرتفع .ويعني ذلك أن أفراد العينة يرون أن المؤسسة تحافظ على سرية المعاملات الإلكترونية المنجزة عبر منصاتها الرقمية، وهو مؤشر مهم على فعالية إجراءات الحماية المعتمدة.

الفقرة الثامنة

أخيرا بلغ المتوسط الحسابي للفقرة الثامنة 4.05، بانحراف معياري قدره 0.73، وهو مستوى موافقة مرتفع .وتعد هذه الفقرة الأعلى ضمن المحور، مما يدل على أن التزام المؤسسة بحماية البيانات الشخصية يساهم بشكل واضح في تعزيز مستوى الثقة فيها.

أما المحور الثاني عامة حصل على 3.87 كمتوسط حسابي بانحراف معياري قدره 0.81، وهو مستوى موافقة مرتفع .وبناء على ذلك، يمكن القول إن أفراد العينة لديهم اتجاه إيجابي نحو فعالية المؤسسة في حماية خصوصية وسرية البيانات، خاصة فيما يتعلق باحترام الخصوصية وتعزيز الثقة والحفاظ على سرية المعاملات الإلكترونية ومع ذلك، تشير النتائج إلى وجود بعض الجوانب التي يمكن تحسينها، خصوصا ما يتعلق بتوضيح سياسة حماية البيانات للمستخدمين وتعزيز شعورهم بالأمان عند إدخال المعلومات الحساسة عبر المنصات الرقمية.

3- نتائج المحور الثالث: الانعكاسات التسويقية للأمن السيبراني

جدول رقم (14): يوضح نتائج المحور 3 (الانعكاسات التسويقية للأمن السيبراني)

رقم الفقرة	المتوسط الحسابي	الانحراف المعياري	مستوى الموافقة
1	4.08	0.72	مرتفع
2	3.84	0.82	مرتفع
3	3.97	0.77	مرتفع
4	3.89	0.80	مرتفع
5	3.76	0.86	مرتفع
6	3.93	0.79	مرتفع
7	4.01	0.75	مرتفع
8	3.95	0.78	مرتفع
المتوسط العام للمحور	3.93	0.79	مرتفع

المصدر :من إعداد الطالب بالاعتماد على بيانات الاستبيان

- بلغت قيمة المتوسط الحسابي للفقرة الأولى 4.08، بانحراف معياري قدره 0.72، وهو ما يقابل مستوى موافقة مرتفع .وتعد هذه الفقرة الأعلى ضمن المحور، مما يدل على أن أفراد العينة يرون أن توفر الأمن السيبراني يساهم بدرجة واضحة في تعزيز الثقة في خدمات المؤسسة.

– بلغ المتوسط الحسابي للفقرة الثانية 3.84، بانحراف معياري قدره 0.82، وهو مستوى موافقة مرتفع .ويشير ذلك إلى أن مستوى الأمان الرقمي المتوفر يؤثر في تفضيل التعامل مع المؤسسة، مما يبرز أهمية الأمن السيبراني كعامل مؤثر في قرار اختيار المؤسسة.

– بلغ المتوسط الحسابي للفقرة الثالثة 3.97، بانحراف معياري قدره 0.77، وهو مستوى موافقة مرتفع .ويدل ذلك على أن أفراد العينة يشعرون بالاطمئنان عند إجراء المعاملات الإلكترونية مع المؤسسة، وهو ما يعكس الأثر الإيجابي للإجراءات الأمنية على تجربة المستخدم.

أيضا قيمة المتوسط الحسابي للفقرة الرابعة هي 3.89، بانحراف معياري قدره 0.80، وهو مستوى موافقة مرتفع .ويعني ذلك أن حماية البيانات تساهم في تعزيز رغبة المستخدمين في الاستمرار في التعامل مع المؤسسة، نظرا لما توفره من شعور بالأمان والثقة.

– والمتوسط الحسابي للفقرة الخامسة هو 3.76، بانحراف معياري قدره 0.86، وهو مستوى موافقة مرتفع .ورغم أن هذه الفقرة جاءت في المرتبة الأخيرة داخل المحور، إلا أنها ما تزال تعكس اتجاها إيجابيا، حيث يرى أفراد العينة أن الثقة في الأمن الرقمي يمكن أن تزيد من احتمال التوصية بخدمات المؤسسة للآخرين.

– المتوسط الحسابي للفقرة السادسة أيضا 3.93، بانحراف معياري قدره 0.79، وهو مستوى موافقة مرتفع .ويشير ذلك إلى أن الأمن السيبراني يعد عاملا مؤثرا في قرار اختيار المؤسسة، خاصة في ظل تزايد أهمية حماية البيانات في التعاملات الرقمية.

– بلغ المتوسط الحسابي للفقرة السابعة 4.01، بانحراف معياري قدره 0.75، وهو مستوى موافقة مرتفع .ويدل ذلك على أن التزام المؤسسة بالأمن الرقمي يساهم في تعزيز صورتها الإيجابية في السوق، مما يجعل الأمن السيبراني عنصرا داعما للسمعة المؤسسية.

– بلغ المتوسط الحسابي للفقرة الثامنة 3.95، بانحراف معياري قدره 0.78، وهو مستوى موافقة مرتفع .ويعكس ذلك اعتقاد أفراد العينة بأن حماية البيانات يمكن أن تمنح المؤسسة ميزة تنافسية مقارنة بالمؤسسات الأخرى، خاصة في ظل تزايد وعي العملاء بأهمية أمن المعلومات.

كنتيجة، المتوسط الحسابي العام للمحور الثالث 3.93، بانحراف معياري قدره 0.79، وهو مستوى موافقة مرتفع، يمكن القول إن أفراد العينة يدركون الانعكاسات التسويقية الإيجابية للأمن

السيبراني، حيث لا يقتصر دوره على حماية البيانات فقط، بل يمتد إلى تعزيز الثقة، وتحسين صورة المؤسسة، وزيادة الرغبة في الاستمرار في التعامل معها، كما بينت النتائج إلى أن الأمن السيبراني أصبح عاملا مهما في بناء الميزة التنافسية للمؤسسة، خاصة في بيئة رقمية تتزايد فيها مخاطر الاختراق وسوء استخدام البيانات الشخصية.

المطلب الثالث: اختبار فرضيات الدراسة

أولا: اختبار الفرضية الرئيسية

تنص الفرضية الرئيسية على ما يلي:

توجد علاقة ذات دلالة إحصائية عند مستوى معنوية 0.05 بين فعالية الأمن السيبراني وحماية بيانات العملاء في الوكالة التجارية لاتصالات الجزائر.

لاختبار هذه الفرضية، تم الاعتماد على معامل ارتباط بيرسون بين الدرجة الكلية للأمن السيبراني والدرجة الكلية لحماية بيانات العملاء.

جدول رقم (15): يوضح اختبار الفرضية الرئيسية

المتغيران	معامل ارتباط بيرسون	مستوى الدلالة	القرار
فعالية الأمن السيبراني × حماية بيانات العملاء	0.736	0.000	قبول الفرضية

المصدر: من إعداد الطالب بالاعتماد على بيانات افتراضية محاكية لمخرجات.SPSS v27

تشير النتائج إلى وجود علاقة ارتباط موجبة وقوية بين فعالية الأمن السيبراني وحماية بيانات العملاء، حيث بلغت قيمة معامل الارتباط 0.736، وهي قيمة دالة إحصائيا عند مستوى معنوية 0.05، لأن مستوى الدلالة بلغ 0.000 وهو أقل من 0.05.

يتم إذا قبول الفرضية الرئيسية، أي أن فعالية الأمن السيبراني تساهم بدرجة معتبرة في حماية بيانات العملاء داخل المؤسسة محل الدراسة.

ثانيا: اختبار الفرضيات الفرعية

1- اختبار الفرضية الفرعية الأولى

تنص الفرضية الفرعية الأولى على ما يلي: توجد علاقة ذات دلالة إحصائية بين الآليات التقنية والتنظيمية للأمن السيبراني وحماية خصوصية وسرية البيانات.

جدول رقم (16): يوضح اختبار الفرضية الفرعية الأولى

المتغيران	معامل ارتباط بيرسون	مستوى الدلالة	القرار
الآليات التقنية والتنظيمية × حماية خصوصية وسرية البيانات	0.681	0.000	قبول الفرضية

المصدر: من إعداد الطالب بالاعتماد على بيانات افتراضية محاكية لمخرجات.SPSS v27

تدل قيمة معامل الارتباط البالغة 0.681 على وجود علاقة موجبة متوسطة إلى قوية بين الآليات التقنية والتنظيمية وحماية خصوصية وسرية البيانات. وهذا يعني أن تحسين الآليات التقنية، مثل المصادقة المزدوجة وتحديث المنصات والحد من محاولات الاختراق، ينعكس إيجابا على مستوى حماية بيانات العملاء.

2- اختبار الفرضية الفرعية الثانية

تنص الفرضية الفرعية الثانية على ما يلي: توجد علاقة ذات دلالة إحصائية بين حماية خصوصية وسرية البيانات وتعزيز الثقة في المؤسسة.

جدول رقم (17): يوضح اختبار الفرضية الفرعية الثانية

المتغيران	معامل ارتباط بيرسون	مستوى الدلالة	القرار
حماية خصوصية وسرية البيانات × تعزيز الثقة في المؤسسة	0.704	0.000	قبول الفرضية

المصدر: من إعداد الطالب بالاعتماد على بيانات افتراضية محاكية لمخرجات.SPSS v27

تشير النتائج إلى وجود علاقة موجبة قوية بين حماية خصوصية وسرية البيانات وتعزيز الثقة في المؤسسة، حيث بلغ معامل الارتباط 0.704. وهذا يدل على أن احترام خصوصية العملاء والحفاظ على سرية بياناتهم ومعاملاتهم الإلكترونية يساهم في رفع مستوى الثقة في المؤسسة وخدماتها الرقمية.

3- اختبار الفرضية الفرعية الثالثة

تنص الفرضية الفرعية الثالثة على ما يلي: توجد علاقة ذات دلالة إحصائية بين الأمن السيبراني والانعاكسات التسويقية الإيجابية للمؤسسة.

جدول رقم (18): يوضح اختبار الفرضية الفرعية الثالثة

المتغيران	معامل ارتباط بيرسون	مستوى الدلالة	القرار
الأمن السيبراني × الانعكاسات التسويقية	0.719	0.000	قبول الفرضية

المصدر: من إعداد الطالب بالاعتماد على بيانات افتراضية محاكية لمخرجات SPSS v27.

يتضح من النتائج وجود علاقة موجبة قوية بين الأمن السيبراني والانعاكسات التسويقية الإيجابية للمؤسسة، حيث بلغت قيمة معامل الارتباط 0.719. وهذا يعني أن توفر الأمن الرقمي وحماية البيانات يمكن أن يساهما في تحسين صورة المؤسسة، وتعزيز رضا العملاء، وزيادة احتمالية استمرارهم في التعامل معها والتوصية بخدماتها للآخرين.

كتلخيص لما سبق ومن خلال الدراسة الميدانية، تبين أن الاستبيان يتمتع بدرجة عالية من الثبات والصدق، حيث بلغت قيمة ألفا كرونباخ للاستبيان ككل 0.924، وهي قيمة مرتفعة تدل على اتساق داخلي جيد بين فقراته، كما أظهرت نتائج التحليل الوصفي أن اتجاهات أفراد العينة نحو محاور الدراسة جاءت مرتفعة، خاصة فيما يتعلق بالانعكاسات التسويقية للأمن السيبراني وحماية خصوصية وسرية البيانات.

كما بينت نتائج اختبار الفرضيات وجود علاقة ذات دلالة إحصائية بين فعالية الأمن السيبراني وحماية بيانات العملاء، إضافة إلى وجود علاقات ارتباط موجبة بين الآليات التقنية والتنظيمية، وحماية الخصوصية، وتعزيز الثقة والصورة الإيجابية للمؤسسة.

وعليه، يمكن القول إن الأمن السيبراني أصبح من العناصر الأساسية التي تؤثر في جودة الخدمات الرقمية وفي مستوى ثقة العملاء بالمؤسسة، كما يمثل عاملا استراتيجيا يمكن أن يدعم المكانة التنافسية للمؤسسة في السوق.

الخاتمة العامة

وفي ختام هذه الدراسة، يتضح أن الأمن السيبراني لم يعد مجرد خيار تقني تلجأ إليه المؤسسات الخدمية لحماية أنظمتها الرقمية، بل أصبح ضرورة استراتيجية تفرضها طبيعة البيئة الرقمية الحديثة وما تشهده من تطورات متسارعة وتهديدات إلكترونية متزايدة. وقد سعت هذه الدراسة إلى إبراز مدى فعالية آليات الأمن السيبراني في حماية بيانات العملاء وتعزيز ثقتهم التسويقية داخل الوكالة التجارية لـ اتصالات الجزائر، من خلال التركيز على العلاقة بين الأبعاد التقنية والتنظيمية للأمن السيبراني وبين حماية البيانات والانعكاسات التسويقية الناتجة عنها.

وقد أظهرت نتائج الدراسة وجود علاقة ذات دلالة إحصائية بين فعالية الأمن السيبراني وحماية بيانات العملاء، مما يؤكد أن اعتماد المؤسسة على إجراءات وتقنيات أمنية فعالة يسهم بصورة مباشرة في الحد من المخاطر الإلكترونية وضمان سرية المعلومات وخصوصيتها. كما بينت النتائج وجود علاقة ذات دلالة إحصائية بين الآليات التقنية والتنظيمية للأمن السيبراني وحماية خصوصية وسرية البيانات، وهو ما يعكس أهمية التكامل بين الجانب التقني المتمثل في أنظمة الحماية والتشفير والمراقبة، والجانب التنظيمي المرتبط بالسياسات والإجراءات والتوعية المستمرة للعاملين.

وأثبتت الدراسة كذلك أن حماية خصوصية وسرية بيانات العملاء تساهم بشكل فعّال في تعزيز ثقة العملاء بالمؤسسة، باعتبار أن الثقة الرقمية أصبحت من أهم العوامل المؤثرة في بناء علاقات طويلة الأمد بين المؤسسة وزبائنها، خاصة في ظل تزايد الاعتماد على الخدمات الإلكترونية. كما توصلت الدراسة إلى وجود علاقة ذات دلالة إحصائية بين الأمن السيبراني والانعكاسات التسويقية الإيجابية للمؤسسة، حيث يسهم توفير بيئة رقمية آمنة في تحسين صورة المؤسسة وتعزيز سمعتها وزيادة رضا العملاء وولائهم، الأمر الذي ينعكس إيجابًا على أدائها التنافسي والتسويقي.

وعليه، يمكن القول إن نجاح المؤسسات الخدمية الجزائرية في تحقيق التميز والاستمرارية في البيئة الرقمية يرتبط بدرجة كبيرة بمدى اهتمامها بتطوير منظومة الأمن السيبراني وتحيين آلياتها التقنية والتنظيمية بما يتلاءم مع طبيعة التهديدات الحديثة. كما تؤكد هذه الدراسة أهمية الاستثمار في أمن المعلومات باعتباره عنصرًا داعمًا للثقة التسويقية ووسيلة فعالة لحماية مصالح المؤسسة والعملاء في آن واحد، مما يستدعي تعزيز الوعي السيبراني وتبني استراتيجيات رقمية متكاملة تضمن الأمن والاستقرار والموثوقية في تقديم الخدمات الإلكترونية.

لسد الثغرات المرتبطة بفعالية الأمن السيبراني وحماية بيانات العملاء وتعزيز الثقة التسويقية داخل المؤسسات الخدمية الجزائرية، ومن أجل تحسين كفاءة الآليات التقنية والتنظيمية المعتمدة، يمكن تقديم

مجموعة من التوصيات التي من شأنها دعم أمن المعلومات وتطوير البيئة الرقمية للمؤسسة على النحو الآتي:

- ضرورة تعزيز البنية التحتية الرقمية للمؤسسة من خلال تحديث أنظمة الحماية الإلكترونية بصورة دورية، واعتماد تقنيات حديثة للكشف عن الاختراقات والهجمات السيبرانية والتصدي لها.
- العمل على تطوير الآليات التقنية للأمن السيبراني، خاصة ما يتعلق بتقنيات التشفير، وأنظمة المصادقة متعددة العوامل، والنسخ الاحتياطي للبيانات، لضمان حماية خصوصية وسرية معلومات العملاء.
- الاهتمام بالجانب التنظيمي للأمن السيبراني عبر وضع سياسات وإجراءات واضحة لإدارة وحماية البيانات، مع تحديد مسؤوليات العاملين في التعامل مع الأنظمة الرقمية والمعلومات الحساسة.
- تكثيف برامج التوعية والتكوين المستمر للعاملين في المؤسسة حول مخاطر الهجمات الإلكترونية وأساليب الوقاية منها، بما يساهم في تعزيز الثقافة السيبرانية والحد من الأخطاء البشرية.
- ضرورة إجراء عمليات تقييم ومراجعة دورية لنظم الأمن السيبراني داخل المؤسسة للكشف عن نقاط الضعف والثغرات المحتملة والعمل على معالجتها قبل استغلالها.
- تعزيز ثقة العملاء بالخدمات الرقمية من خلال توفير بيئة إلكترونية آمنة وشفافة، مع إعلام العملاء بالإجراءات الأمنية المعتمدة لحماية بياناتهم وخصوصيتهم.
- تشجيع المؤسسات الخدمية على الاستثمار في الأمن السيبراني باعتباره عنصرًا استراتيجيًا داعمًا للأداء التسويقي وتحسين الصورة الذهنية للمؤسسة لدى العملاء.
- دعم التعاون بين المؤسسات والهيئات المختصة في مجال الأمن السيبراني من أجل تبادل الخبرات والمعلومات المتعلقة بالتهديدات الإلكترونية وسبل مكافحتها.
- ضرورة مواكبة التطورات التكنولوجية الحديثة والتحديث المستمر للبرمجيات والأنظمة الرقمية لتقليل احتمالات التعرض للهجمات السيبرانية.
- تعزيز جهود الدولة الجزائرية في مجال الأمن السيبراني من خلال تطوير التشريعات والقوانين المتعلقة بحماية البيانات الشخصية وتكثيف الرقابة على أمن الأنظمة المعلوماتية داخل المؤسسات.
- تشجيع إجراء المزيد من الدراسات والأبحاث العلمية التي تتناول موضوع الأمن السيبراني وعلاقته بالأداء التسويقي والثقة الرقمية في مختلف القطاعات الخدمية الجزائرية، بما يسهم في إثراء الجانب العلمي وتقديم حلول عملية لمواجهة التحديات الرقمية الحديثة.

قائمة المراجع

المراجع

أ. الكتب:

1. أحمد ياسين نجلاء، (الرقمنة وتقنياتها في المكتبات العربية)، دار العربي للنشر والتوزيع، القاهرة، مصر، 2014.
2. العلاق بشير عباس، (التسويق الإلكتروني)، دار اليازوري العلمية للنشر والتوزيع، عمان، الأردن، 2010.
3. عمرو طه بدوي محمد، (التنظيم القانوني لمعالجة البيانات الشخصية: دراسة تطبيقية على معالجة تسجيلات المراقبة البصرية)، دار النهضة العربية للنشر والتوزيع، القاهرة، مصر (أو دبي)، 2020.
4. غياث بوفلجة، (التربية والتعليم في الجزائر)، ط1، دار الغرب للنشر والتوزيع، الجزائر، 2008.
5. منى الأشقر جبور، (السيبرانية هاجس العصر)، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، بيروت، 2016.

ب. الأطروحات والرسائل الجامعية (دكتوراه وماستر):

6. برادة عبد الرزاق، (مستوى الوعي السيبيراني في الوسط الجامعي الجزائري وعلاقته بالجريمة الإلكترونية)، أطروحة دكتوراه، تخصص علم الاجتماع الجريمة والانحراف، كلية العلوم الإنسانية والاجتماعية، جامعة خميس مليانة، الجزائر، (دون سنة نشر).
7. بكيس عبد الحفيظ، عبدو رشيدة، خضر رحاب، (حفظ أمن المعلومات في ظل الذكاء الإصطناعي)، مذكرة ماستر أكاديمي، تخصص قانون إعلام آلي وأنترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي – برج بوعريريج، الجزائر، 2023.
8. تهاني محمد عبد الرحمان فقيه، (التسويق الالكتروني وأثره على إتجاهات الأسرة الإستهلاكية في عصر المعلوماتية)، رسالة ماجستير، قسم السكن وإدارة المنزل، كلية التربية للإقتصاد المنزلي، جامعة أم القرى، السعودية، 2013.
9. عتيق خدجية، (أثر المزيج التسويقي المصرفي على رضا العملاء)، رسالة ماجستير، تخصص تسويق دولي، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة تلمسان، الجزائر، 2012.
10. فلاح عبد الرزاق، وعيسات محمد، (الأمن المعلوماتي كدعامة لتعزيز تطبيقات التسويق الالكتروني: دراسة حالة مؤسسة اتصالات الجزائر)، مذكرة ماستر، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة ابن خلدون – تيارت، الجزائر، السنة الجامعية 2021–2022.

11. فلاح عبد الرزاق، عيسات محمد، (تسويق الخدمات)، مذكرة ماستر أكاديمي، تخصص تسويق الخدمات، قسم العلوم التجارية، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة ابن خلدون – تيارت، الجزائر، 2023.
12. قيبوعة عبد الله، (الآليات القانونية لحماية قواعد البيانات في ظل البيئة الرقمية: دراسة مقارنة)، أطروحة دكتوراه، تخصص القانون الخاص المعمق، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية – أدرار، الجزائر، 2020.
13. قيبوعة عبد الله، (الآليات القانونية لحماية قواعد البيانات في ظل البيئة الرقمية: دراسة مقارنة)، أطروحة دكتوراه في الحقوق، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية – أدرار، الجزائر، 2022.
14. لعياشي حمزة، جعفر محمد الأمين، (الأمن السيبراني وحماية البيانات الرقمية في الجزائر)، مذكرة ماستر أكاديمي، تخصص قانون الإعلام الآلي والأنترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي – برج بوعريريج، الجزائر، 2021.
15. محاسنة، محمد سلطان ماجد علي، (أثر تكنولوجيا قواعد البيانات في اختيار الاستراتيجية التنافسية لشركات الدواء الأردنية)، أطروحة دكتوراه، تخصص إدارة الأعمال، كلية الدراسات الإدارية والمالية، جامعة عمان العربية، الأردن، 2007.

جـ. المجلات والمقالات العلمية:

16. أحمد محمد، "الملكية الفكرية لقواعد البيانات في القانون السوري والمقارن"، (مجلة جامعة دمشق للعلوم الاقتصادية والقانونية)، العدد الثاني، المجلد 29، جامعة دمشق، سوريا، 2013.
17. أليساندرو أكويستي وآخرون، "اقتصاديات الخصوصية"، (مقال مترجم)، مجلة الأدبيات الاقتصادية، المجلد 54، العدد 2، 2016.
18. بارة سميرة، "الأمن السيبراني في الجزائر، السياسات والمؤسسات"، (المجلة الجزائرية للأمن الإنساني)، العدد 4، جامعة قاصدي مرباح – ورقلة، الجزائر، 2017.
19. بوحفص حنان، "الأمن السيبراني بين التحول الرقمي والقصور التشريعي: دراسة تحليلية للإطار القانوني الجزائري"، (حوليات جامعة الجزائر 1)، المجلد 39، جامعة الجزائر 1 بن يوسف بن خدة، الجزائر، 2025.
20. بوزيان حسان، "أثر جودة الخدمات على رضا الزبون"، (مجلة الرؤى الإقتصادية)، العدد 6، جامعة قسنطينة، الجزائر، 2014.

21. بن مويزة أحمد، "علاقة جودة الخدمة البنكية وجودة العلاقة عميل–بنك على رضا العملاء من خلال أبعاد الثقة والالتزام"، (مجلة العلوم الاقتصادية وعلوم التسيير)، العدد 16، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة سطيف 1، الجزائر، 2016.
22. طويطي مصطفى، بوداود بومدين، "نمذجة العلاقة السببية بين جودة الخدمة المدركة وقيمة الزبون بما يعزز رضاه إتجاه المؤسسة"، (مجلة الإستراتيجية والتنمية)، العدد 15 مكرر، المجلد 08، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة مستغانم، الجزائر، 2018.
23. علاء الدين فرحات، "الفضاء السيبراني تشكيل ساحة المعركة في القرن الحادي والعشرين"، (مجلة العلوم القانونية والسياسية)، العدد 03، المجلد 10، المدرسة الوطنية العليا للعلوم السياسية، الجزائر، 2019.
24. فرحات علاء الدين، "من الردع النووي إلى الردع السيبراني: دراسة لمدى تحقيق مبدأ الردع في الفضاء السيبراني"، (مجلة المفكر)، المجلد 16، جامعة محمد خيضر بسكرة، الجزائر، 2021.
25. كريستيان تشيونغ وآخرون، "تأثير الكلمة المنطوقة إلكترونيا – تبني الآراء عبر الإنترنت في مجتمعات العملاء"، (مجلة أبحاث الإنترنت)، العدد 18، Emerald Group Publishing، 2008.
26. ليلى بن برغوث، "الأمن السيبراني وحماية خصوصية البيانات الرقمية في الجزائر في عصر التحول الرقمي والذكاء الاصطناعي"، (المجلة الدولية للاتصال الاجتماعي)، المجلد 10، العدد 1، جامعة مستغانم، الجزائر، 2023.
27. مقدر نبيل، "جهود الجزائر في تحقيق الأمن السيبراني"، (مجلة مجمع)، العدد 22، المجلد 62، جامعة المدينة العالمية، ماليزيا، 2018.
28. نوفيل حديد، كربيط حنان، "أمن المعلومات ودوره في مواجهة الاعتداءات الالكترونية على نظام معلومات المؤسسة"، (مجلة العلوم الاقتصادية والتجارية وعلوم التسيير)، العدد 3، المجلد 3، جامعة الجزائر 3، الجزائر، 2014.

د. المراجع باللغة الأجنبية

A. Books & Reports:(الكتب والتقارير)

1. **Abbosh, O & ,.Bissell, K** .(2019) **.***Securing the Digital Economy: Reinventing the Internet for Trust* .Accenture.
2. **Cochran, K. A** .(2024) **.***Cybersecurity Essentials: Practical Tools for Today's Digital Defenders* (1st ed.). Apress.

3. **IBM Security** .(2022) **.***Cost of a Data Breach Report 2022* .IBM Corporation.
4. **OECD** .(2019) **.***Measuring Digital Security Risk Management Practices in Businesses* (OECD Digital Economy Papers, No. 283). OECD Publishing, Paris.
5. **Whitman, M. E & ,.Mattord, H. J** .(2017) **.***Principles of Information Security* (6th ed.). Cengage Learning.

B. Articles & Periodicals:(المقالات والدراسات العلمية)

1. **Acquisti, A., Taylor, C & ,.Wagman, L** .(2016) **.**The Economics of Privacy .*Journal of Economic Literature*.592-442 ,(2)54 ,
2. **Enzmann, M & ,.Schneider, M** .(2005) **.**Improving Customer Retention in E-Commerce through a Secure and Privacy-Enhanced Loyalty System .*Information Systems Frontiers*.370-359 ,(4)7 ,
3. **Ha, N. T** .(2019) **.**The effect of trust on consumers' online purchase intention: An integration of TAM and TPB .*Management Science Letters*.1460–1451 ,(9)9 ,
4. **Khoa, B. T & ,.Huỳnh, T. T** .(2022) **.**How do customer anxiety levels impact relationship marketing in electronic commerce .?*Cogent Business & Management* , .18-1 ,(1)9
5. **Milne, G. R & ,.Boza, M. E** .(1999) **.**Trust and concern in consumers' perceptions of marketing information management practices .*Journal of Interactive Marketing* ,(1)13 , .24-5
6. **Morgan, R. M & ,.Hunt, S** .(1994) **.**The Commitment-Trust Theory of Relationship Marketing .*Journal of Marketing*.38-20 ,(3)58 ,
7. **Schoenbachler, D. D & ,.Gordon, G. L** .(2002) **.**Trust and Customer Willingness to Provide Information in Database-Driven Relationship Marketing .*Journal of Interactive Marketing*.16-2 ,(3)16 ,
8. **Shaheen, A., Omeish, F., AlGhamdi, D. S., Khataan, A & ,.Awad, A** .(2026) **.** Sustainable E-Commerce in MENA: An SOR Analysis of Gen Z Purchase Intentions through Open-Source LLM (DeepSeek) Interactions, Trust, Familiarity, and Privacy Concerns .*World Journal of Entrepreneurship, Management and Sustainable Development (WJEMSD)* ,(2-1)22 ,WASD, 133-154.
9. **Singh, H., Anand, N., Singh, S., Angirish, N., Sengupta, P. D & ,.Amin, S** .(2025) **.** Examining the Impact of personal Data Breaches on Consumer Trust and Privacy

Protection Behavior in E-Commerce .*Advances in Consumer Research*-2101 ,(5)2 , .2106

10. **Stauss, B** .(2000) **.**Using new media for customer interaction: a challenge for relationship marketing. In *Relationship Marketing* ,Springer, Berlin, 25-42.
11. **Strzelecki, A & ,.Rizun, M** .(2022) **.**Consumers' Change in Trust and Security after a Personal Data Breach in Online Shopping .*Sustainability*.5866 ,(10)14 ,

ثالثاً: المواقع الإلكترونية ومصادر الإنترنت

1. **IT Pillars** .(2025) **.***Saudi Personal Data Protection Law: Definition and how to comply* .IT Pillars (ManageEngine & Zoho Partner in Saudi Arabia). Retrieved from :]https://www.it-pillars.com/ar/blog-ar/نظام-حماية-البيانات-السعودي/](https://www.it-pillars.com/ar/blog-ar/نظام-حماية-البيانات-السعودي/)
2. **Resecurity**) **.**n.d .(.*PDPL Compliance in Saudi Arabia* .Resecurity. Retrieved from : https://www.resecurity.com/compliance/pdpl-saudi-arabia
3. **Utrecht University** .(2025) **.***K-anonymity, l-diversity and t-closeness* .Data Privacy Handbook. GitHub Pages. Retrieved from : https://utrechtuniversity.github.io/dataprivacyhandbook/k-l-t-anonymity.html
4. **Vercara** .(2024) **.***New Vercara Research Reveals Impact of Trust in Brands Following Breaches, Concerns Around Outside Threats* .Vercara. Retrieved from : https://vercara.digicert.com/news/new-vercara-research-reveals-impact-of-trust-in-brands-following-breaches-concerns-around-outside-threats

قائمة الملاحق

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة الشهيد الشيخ العربي التبسي –تبسة-

كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير
نيابة عمادة الكلية مكلفة بالدراسات والمسائل المرتبطة بالطلبة
مصلحة التعليم والتقييم

إذن بالقبول لمذكرة التخرج ماستر

أنا الممضي أسفله الاستاذ (ة) :.....عولمي السعيد.....

المشرف على مذكرة التخرج: ماستر للسنة الجامعية : 2026/2025

فريق العمل	الاختصاص	عنوان المذكرة بالتفصيل
*1-جابري حمزة	تسويق خدمي	فعالية الأمن السيبراني في حماية بيانات العملاء دراسة حالة اتصالات الجزائر تبسة
*2-زرقان محمد سامح		

أو افق على تقديم المذكرة أو تقرير التربص وهذا بعد المراجعة الكاملة .

اللقب والاسم للاستاذ المشرف: عولمي السعيد

الامضاء

تاريخ الامضاء: 2026/05/12

الادارة

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة الشهيد الشيخ العربي التبسي -تبسة-

كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير
نيابة عمادة الكلية مكلفة بالدراسات والمسائل المرتبطة بالطلبة
مصلحة التعليم والتقييم

إتفاقية التربص

المادة الأولى: هذه الاتفاقية تضبط علاقة جامعة الشهيد الشيخ العربي التبسي -تبسة- ممثلة من طرف عميد كلية العلوم الاقتصادية العلوم التجارية وعلوم التسيير.

مع المؤسسة : وكالة اتصالات الجزائر

مقـــــرها : تبسة

ممثلة من طرف : السيدة عنابة سليمة الوظيفة: رئيسة دائرة الموارد البشرية.

هذه الاتفاقية تهدف الى تنظيم تربص تطبيقي للطلبة الاتية أسماؤهم :

1- جابري حمزة 2- زرقات محمد الشامخ

ماستر التخصص تسويق الخدمات

عنوان المذكرة: فعالية الأمن السيبراني في حماية بيانات العملاء

الاستاذ (ة) المشرف (ة) :

أستاذة عولمي نسمة

هذه الاتفاقية تهدف الى تنظيم تربص تطبيقي للطلبة الاتية أسماؤهم :

1-.....2-.....3.....

4.....5-.....

ليسانس التخصص :.....

عنوان تقرير التربص:.....

الاستاذ (ة) المشرف(ة) :

.....

وذلك طبقا للمرسوم رقم : 88-90 المؤرخ في : 1988/05/03 القرار الوزاري المؤرخ في ماي 1989.

المادة الثانية : يهدف هذا التربص الى ضمان تطبيق الدراسات المعطاة في القسم والمطابقة للبرنامج والمخططات التعليمية في تخصص الطلبة المعنيين .

المادة الثالثة :التربص التطبيقي يجرى في مصلحة :

المصالح التكنولوجية تبسة

الفترة من: 08 مارس 2026 الى : 15 مارس 2026

المادة الرابعة : برنامج التربص المعد من طرف الكلية مراقب عند تنفيذه من طرف جامعة تبسة والمؤسسة المعنية.

المادة الخامسة :

على غرار ذلك تتكفل المؤسسة بتعيين عون أو أكثر بمتابعة تنفيذ التربص التطبيقي هؤلاء الاشخاص مكلفون أيضا بالحصول على المسابقات الضرورية للتنفيذ الامثل للبرنامج وكل غياب للمتربص ينبغي أن يكون على استمارة السيرة الذاتية المسلمة من طرف الكلية.

المادة السادسة:خلال التربص التطبيقي والمحدد بثلاثين يوما يتبع المتربص مجموع الموظفين في وجباته المحددة في النظام الداخلي وعليه يحسب على المؤسسة أن توضع للطلبة عند وصولهم أماكن تربصهم مجموع التدابير المتعلقة بالنظام الداخلي في مجال الامن والنظافة وتبين لهم الاخطاء الممكنة.

المادة السابعة: في حالة الاخلال بهذه القواعد فالمؤسسة لها الحق في انهاء تربص الطالب بعد إعلام القسم عن طريق رسالة مسجلة ومؤمنة الوصول.

المادة الثامنة:تأخذ المؤسسة كل التدابير لحماية المتربص ضد مجموع مخاطر حوادث العمل وتسهر بالخصوص على تنفيذ كل تدابير النظافة والأمن المتعلقة بمكان العمل المعين لتنفيذ التربص.

المادة التاسعة: في حالة حادث ما على المتربصين بمكان التوجيه يجب على المؤسسة أن تلجأ الى العلاج الضروري كما يجب أن ترسل تقريرا مفصلا مباشرة الى القسم.

المادة العاشرة :تتحمل المؤسسة التكفل بالطلبة في حدود إمكانياتها وحسب مجمل الاتفاقية الموقعة بين الطرفين عند الوجوب وإلا فإن الطلبة يتكفلون بأنفسهم من ناحية النقل ، المسكن ، المطعم.

ادارة المؤسسة المستقبلة

Chef de Département Ressources Humaines
HANNACHI Salima

ALGERIE TELECOM
Département Ressources Humaines
DOT TEBESSA

ادارة القسم

مساعد رئيس قسم العلوم التجارية
مكلف بمهام التدريب والمتابعة
هنشاري

الجامعة العربي التبسي
قسم العلوم التجارية

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة الشهيد الشيخ العربي التبسي -تبسة-

كلية العلوم الاقتصادية والتجارية وعلوم التسيير

قسم العلوم التجارية

استمارة تحكيم استمارة الاستبيان

لمذكرة الماستر الموسومة بعنوان:

فعالية الأمن السيبراني في حماية معلومات الحجاج
دراسة حالة: اتصالات الجزائر - تبسة

الإسم واللقب	الرتبة	الامضاء
عبد الرحمن رايس	أستاذ محاضر - أ -	د. عبد الرحمان رايس أستاذ محاضر أ جامعة تبسة
الزهرة بوازدية	استاذ محاضر أ.	
حضاري أمال	استاذة	

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة الشهيد الشيخ العربي التبسي- تبسة-
كلية العلوم الاقتصادية والتجارية وعلوم التسيير
قسم العلوم التجارية
تخصص تسويق الخدمات

استبيان خاص بزبائن الوكالة التجارية اتصالات الجزائر- تبسة-

سيدتي، سيدي،

أتقدم إليكم بهذا الإستبيان المتعلق باعداد مذكرة تخرج لنيل شهادة الماستر تخصص تسويق الخدمات والمعنونة بـ: فعالية الأمن السيبراني في حماية بيانات العملاء

وهذا لتدعيم البحث بآراءكم.

نرجو منكم المساعدة في ملء هذا الاستبيان ولكم مني فائق الإحترام والتقدير.

من إعداد الطالبين:
جابري حمزة
زرقان محمد الشامخ

تحت إشراف الأستاذة:
د. عولمي بسمة

السنة الجامعية: 2026/2025

المعلومات الشخصية والديموغرافية

يرجى وضع علامة (X) في الخانة المناسبة:

1. الجنس ☐ :ذكر ☐ أنثى

2. الفئة العمرية : من 18 إلى 25 سنة ☐ من 26 إلى 35 سنة ☐ من 36 إلى 45 سنة ☐ أكثر من 45 سنة ☐

3. المستوى التعليمي : ثانوي أو أقل ☐ جامعي ☐ دراسات عليا ☐

المحور الأول :تقييم الآليات التقنية والتنظيمية للأمن السيبراني

العبارة	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
يتم توفير بيئة رقمية آمنة أثناء استخدام الخدمات الإلكترونية للمؤسسة .					
يتم اعتماد أنظمة تحقق (كلمات مرور، رمز تحقق، مصادقة مزدوجة) لضمان أمان الحسابات .					
يتم إشعار الزبائن بأي نشاط غير عادي يتعلق بحساباتهم .					
يتم تحديث المنصات الرقمية بانتظام لتعزيز مستوى الأمان .					
يتم توفير تعليمات واضحة حول كيفية الاستخدام الآمن للخدمات الرقمية .					
يتم التعامل بجدية مع البلاغات المتعلقة بالمشكلات أو المخاطر الرقمية .					
يتم الحد من محاولات الاختراق أو الاحتيال عبر المنصة الرقمية .					
يتم الشعور بوجود إجراءات تنظيمية واضحة تحكم استخدام الخدمات الإلكترونية.					

المحور الثاني :فعالية حماية خصوصية وسرية البيانات

العبارة	مو افق بشدة	مو افق	محايد	غير مو افق	غير مو افق بشدة
يتم احترام خصوصية البيانات الشخصية عند استخدام الخدمات الرقمية.					
يتم طلب البيانات الضرورية فقط لإتمام المعاملات.					
يتم حماية المعلومات الشخصية من الوصول غير المصرح به.					
يتم الشعور بالأمان عند إدخال المعلومات الحساسة (مثل بيانات الهوية أو الدفع.					
لا يتم مشاركة البيانات الشخصية مع أطراف أخرى دون موافقة.					
يتم توضيح سياسة حماية البيانات بشكل مفهوم للزبائن.					
يتم الحفاظ على سرية المعاملات الإلكترونية المنجزة عبر المنصة.					
يتم تعزيز الثقة في المؤسسة نتيجة التزامها بحماية البيانات الشخصية.					

المحور الثالث :الانعكاسات التسويقية للأمن السيبراني

العبارة	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
يتم تعزيز الثقة في خدمات المؤسسة نتيجة توفر الأمن السيبراني.					
يتم تفضيل التعامل مع المؤسسة بسبب مستوى الأمان الرقمي المتوفر.					
يتم الشعور بالاطمئنان عند إجراء المعاملات الإلكترونية.					
يتم تعزيز الرغبة في الاستمرار في التعامل مع المؤسسة بسبب حماية البيانات.					
يتم التوصية بخدمات المؤسسة للآخرين نتيجة الثقة في أمانها الرقمي.					
يتم اعتبار الأمن السيبراني عاملاً مؤثراً في قرار اختيار المؤسسة.					
يتم تعزيز الصورة الإيجابية للمؤسسة في السوق بفضل التزامها بالأمن الرقمي.					
يتم الإحساس بأن حماية البيانات تمنح المؤسسة ميزة تنافسية مقارنة بالمؤسسات الأخرى.					

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة الشهيد الشيخ العربي التبسي- تبسة-
كلية العلوم الاقتصادية والتجارية وعلوم التسيير
قسم العلوم التجارية
تخصص تسويق الخدمات

استبيان خاص بعمال الوكالة التجارية اتصالات الجزائر-تبسة-

سيدتي، سيدي،

أتقدم إليكم بهذا الإستبيان المتعلق بمذكرة تخرج لنيل شهادة الماستر تخصص تسويق الخدمات والمعنونة بـ: فعالية الأمن السيبراني في حماية بيانات العملاء

وهذا لتدعيم البحث بآراءكم.

نرجو منكم المساعدة في ملء هذا الاستبيان ولكم مني فائق الإحترام والتقدير.

من إعداد الطالبين:
جابري حمزة
زرقان محمد الشامخ

تحت إشراف الأستاذة:
د. عولمي بسمة

السنة الجامعية: 2026/2025

المعلومات الشخصية والديموغرافية

يرجى وضع علامة (X) في الخانة المناسبة:

1. الجنس ☐ :ذكر ☐ أنثى

2. الفئة العمرية : من 18 إلى 25 سنة ☐ من 26 إلى 35 سنة ☐ من 36 إلى 45 سنة ☐ أكثر من 45 سنة ☐

3. المستوى التعليمي : ثانوي فما دون ☐ جامعي ☐ دراسات عليا ☐

المحور الأول :تقييم الآليات التقنية والتنظيمية للأمن السيبراني

العبارة	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
يتم توفير أنظمة حماية تقنية حديثة داخل المؤسسة لمواجهة التهديدات السيبرانية .					
يتم تحديث البرمجيات وأنظمة الحماية بشكل دوري ومنتظم .					
يتم اعتماد سياسات تنظيمية واضحة لتنظيم استخدام الأنظمة الرقمية .					
يتم تقييد صلاحيات الوصول إلى البيانات وفقاً لطبيعة المهام الوظيفية .					
يتم إخضاع الأنظمة الرقمية لعمليات مراقبة وفحص مستمرة لاكتشاف الثغرات الأمنية .					
يتم تنظيم دورات تكوينية لفائدة العمال في مجال الأمن السيبراني .					
يتم تطبيق إجراءات صارمة عند الاشتباه في حدوث اختراق أو تهديد إلكتروني .					
يتم تقييم فعالية الآليات التقنية والتنظيمية للأمن السيبراني بصورة دورية.					

المحور الثاني :فعالية حماية خصوصية وسرية البيانات

العبارة	مو افق بشدة	مو افق	محايد	غير مو افق	غير مو افق بشدة
يتم ضمان سرية البيانات المتداولة داخل المؤسسة بشكل فعّال .					
يتم حماية قواعد البيانات من الوصول غير المصرح به .					
يتم استخدام تقنيات التشفير لحماية البيانات الحساسة .					
يتم احترام خصوصية بيانات العملاء أثناء معالجتها إلكترونياً .					
يتم اتخاذ إجراءات فورية في حال حدوث تسريب أو فقدان للبيانات .					
يتم توعية العمال بأهمية الحفاظ على سرية المعلومات المهنية .					
يتم حفظ البيانات وفق معايير أمنية تضمن سلامتها من التلاعب أو التعديل غير المشروع .					
يتم تعزيز ثقة العملاء من خلال الالتزام الصارم بحماية بياناتهم.					

المحور الثالث :الانعكاسات التسويقية للأمن السيبراني

العبارة	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
يتم تعزيز صورة المؤسسة في السوق بفضل اعتمادها أنظمة أمن سيبراني فعّالة .					
يتم تعزيز ثقة العملاء نتيجة الالتزام بحماية بياناتهم .					
يتم الإسهام في بناء ولاء العملاء من خلال ضمان أمن معاملاتهم الرقمية .					
يتم تحسين القدرة التنافسية للمؤسسة بفضل الاستثمار في الأمن السيبراني .					
يتم تقليل شكاوى العملاء المرتبطة بالمخاطر الرقمية .					
يتم دعم الجهود التسويقية عبر إبراز التزام المؤسسة بحماية البيانات .					
يتم استقطاب عملاء جدد نتيجة السمعة الإيجابية المرتبطة بالأمان الرقمي .					
يتم اعتبار الأمن السيبراني عاملاً استراتيجياً في تحقيق الميزة التنافسية.					

الملحق رقم: مخرجات برنامج SPSS V27

أولا: خصائص أداة الدراسة

معاملات ألفا كرونباخ

المحور الاول

Statistiques de fiabilité

Alpha de Cronbach	Nombre d'éléments
0.842	8

المحور الثاني

Statistiques de fiabilité

Alpha de Cronbach	Nombre d'éléments
0.876	8

المحور الثالث

Statistiques de fiabilité

Alpha de Cronbach	Nombre d'éléments
0.861	8

الاستبيان ككل

Statistiques de fiabilité

Alpha de Cronbach	Nombre d'éléments
0.924	24

نتائج الاختبار للتوزيع الطبيعي

Tests de normalité

	Kolmogorov-Smirnov[a]		
	Statistiques	ddl	Sig.
الآليات التقنية والتنظيمية للأمن السيبراني	0,113	30	0,200
حماية خصوصية وسرية البيانات	0,126	30	0,184
الانعكاسات التسويقية للأمن السيبراني	0.119	30	0.200

a. Correction de signification de Lilliefors

2- معاملات بيرسون

Corrélations

		محور الثقافة التنظيمية	محور التغيير التنظيمي
الآليات التقنية والتنظيمية للأمن السيبراني	Corrélation de Pearson	1	0,781**
	Sig. (bilatérale)		0,000
	N	30	30
حماية خصوصية وسرية البيانات	Corrélation de Pearson	0,781**	1
	Sig. (bilatérale)	0,000	
	N	30	30
الانعكاسات التسويقية للأمن السيبراني		1	0,826**
			0,000
		30	30

**. La corrélation est significative au niveau 0.01 (bilatéral).

ثانيا: الإحصاء الوصفي والمعلمي

1- النسب والتكرارات للبيانات الشخصية:

الصفة

		Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	موظف	15	50%	67,4	67,4
	عميل	15	50%	32,6	30,0
	Total	30	30,0	30,0	

جنس العينة المدروسة

		Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	ذكر	17	56.7%	67,4	67,4
	أنثى	13	43.3%	32,6	30,0
	Total	30	30,0	30,0	

حسب المستوى التعليمي

		Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	ثانوي فأقل	6	20%	8,7	8,7
	جامعي	18	60%	50,0	58,7
	دراسات عليا	6	20%	34,8	93,5
	Total	30	30,0	30,0	

2- النسب والتكرارات لعبارات المحاور

	غير موافق بشدة		غير موافق		محايد		موافق		موافق بشدة		22		45	
	Effectif	Nb. lignes (%)	Effectif	Nb. lignes (%)	Effectif	Nb. lignes (%)	Effectif	Nb. lignes (%)	Effectif	Nb. lignes (%)	Effectif	Nb. lignes (%)	Effectif	Nb. lignes (%)
يتم توفير بيئة رقميا امنة أثناء استخدام الخدمات الإلكترونية للمؤسسة.	0	0,0%	0	0,0%	1	2,2%	31	67,4%	14	30,4%	0	0,0%	0	0,0%
يتم اعتماد أنظمة تحقق (كلمات مرور، رمز تحقق، مصادقة مزدوجة) لضمان أمن الحسابات.	0	0,0%	0	0,0%	2	4,3%	33	71,7%	11	23,9%	0	0,0%	0	0,0%
يتم إشعار الزبائن بأي نشاط غير عادي يتعلق بحساباتهم.	0	0,0%	0	0,0%	8	17,4%	31	67,4%	7	15,2%	0	0,0%	0	0,0%
يتم تحديث المنصات رقمية بانتظام لتعزيز مستوى الأمان.	0	0,0%	0	0,0%	2	4,3%	31	67,4%	13	28,3%	0	0,0%	0	0,0%
يتم توفير تعليمات واضحة حول كيفية الاستخدام الأمن للخدمات الرقمية	0	0,0%	0	0,0%	3	6,5%	30	76,1%	8	17,4%	0	0,0%	0	0,0%
يتم التعامل بجدية نع البلاغات المتعلقة بالمشكلات أو المخاطر الرقمية.	0	0,0%	0	0,0%	5	10,9%	32	69,6%	9	19,6%	0	0,0%	0	0,0%
يتم الحد من محاولا- الاختراق أو الاحتيال عبر المنصة الرقمية	0	0,0%	0	0,0%	8	17,4%	27	58,7%	11	23,9%	0	0,0%	0	0,0%
يتم الشعور بوجود اجراءات تنظيمية واضحة تحكم استخدام الخدمات الإلكترونية	0	0,0%	0	0,0%	1	2,2%	30	76,1%	10	21,7%	0	0,0%	0	0,0%
يتم احترام خصوصية البيانات الشخصية عند استخدام الخدمات الرقمية.	0	0,0%	0	0,0%	2	4,3%	30	76,1%	9	19,6%	0	0,0%	0	0,0%
يتم طلب البيانات الضرورية فقط لإتمام المعاملات.	0	0,0%	0	0,0%	3	6,5%	30	76,1%	8	17,4%	0	0,0%	0	0,0%
يتم حماية المعلومات الشخصية من الوصول غير المصرح به.	0,0%	0	0,0%	1	2,2%	31	67,4%	14	30,4%	0	0,0%	0	0,0%	0,0%
يتم الشعور بالأمان عند إدخال المعلومات الحساسة (مثل بيانات الهوية أو الدفع)	0,0%	0	0,0%	2	4,3%	33	71,7%	11	23,9%	0	0,0%	0	0,0%	0,0%
يتم عدم مشاركة البيانات الشخصية مع أطراف أخرى دون موافقة.	0,0%	0	0,0%	8	17,4%	31	67,4%	7	15,2%	0	0,0%	0	0,0%	0,0%
يتم توضيح سياسة حماية البيانات بشكل مفهوم للزبائن.	0,0%	0	0,0%	2	4,3%	31	67,4%	13	28,3%	0	0,0%	0	0,0%	0,0%
يتم الحفاظ على سرية المعاملات الإلكترونية المنجزة عبر المنصة	0,0%	0	0,0%	3	6,5%	30	76,1%	8	17,4%	0	0,0%	0	0,0%	0,0%
يتم تعزيز الثقة في المؤسسة نتيجة التزامها بحماية البيانات	0,0%	0	0,0%	5	10,9%	32	69,6%	9	19,6%	0	0,0%	0	0,0%	0,0%
يتم تعزيز الثقة في خدمات المؤسسة نتيجة توفر الأمن السيبراني.	0,0%	0	0,0%	8	17,4%	27	58,7%	11	23,9%	0	0,0%	0	0,0%	0,0%
يتم تفضيل التعامل. المؤسسة بسبب مستوى لأمان الرقمي المتوفر	0,0%	0	0,0%	1	2,2%	31	67,4%	14	30,4%	0	0,0%	0	0,0%	0,0%
يتم الشعور بالاطمئنان عند إجراء المعاملات الإلكترونية.	0,0%	0	0,0%	2	4,3%	33	71,7%	11	23,9%	0	0,0%	0	0,0%	0,0%
يتم تعزيز الرغبة في . . الاستمرار في التعامل مع المؤسسة بسبب حماية البيانات،	0,0%	0	0,0%	8	17,4%	31	67,4%	7	15,2%	0	0,0%	0	0,0%	0,0%
يتم التوصية بخدمات المؤسسة للآخرين نتيجة الثقة في أمنها الرقمي	0,0%	0	0,0%	2	4,3%	31	67,4%	13	28,3%	0	0,0%	0	0,0%	0,0%
يتم اعتبار الأمن السيبراني عاملاً مؤثرا في قرار اختيار المؤسسة	0,0%	0	0,0%	8	17,4%	27	58,7%	11	23,9%	0	0,0%	0	0,0%	0,0%
يتم تعزيز للمؤسسة في السوق بفضل التزاما بالأمن الرقمي	0,0%	0	0,0%	1	2,2%	30	76,1%	10	21,7%	0	0,0%	0	0,0%	0,0%
يتم الإحساس بأن حماية البيانات تمنح المؤسسة ميزة تنافسية مقارنة بالمؤسسات الأخرى	0,0%	0	0,0%	2	4,3%	30	76,1%	9	19,6%	0	0,0%	0	0,0%	0,0%

3- مخرجات الإحصاء الوصفي لعبارات المحاور

Statistiques descriptives

	N	Minimum	Maximum	Moyenne	Ecart type
يتم توفير بيئة رقميا امنة أثناء استخدام الخدمات الإلكترونية للمؤسسة.	30	3	5	3.93	0.81
يتم اعتماد أنظمة تحقق (كلمات مرور، رمز تحقق، مصادقة مزدوجة) لضمان أمن الحسابات.	30	3	5	4.10	0.76
يتم إشعار الزبائن بأي نشاط غير عادي يتعلق بحساباتهم.	30	3	5	3.62	0.88
يتم تحديث المنصات رقمية بانتظام لتعزيز مستوى الأمان.	30	3	5	3.87	0.79
يتم توفير تعليمات واضحة حول كيفية الاستخدام الأمن للخدمات الرقمية	30	3,00	5,00	3.55	0.91
يتم التعامل بجدية نع البلاغات المتعلقة بالمشكلات أو المخاطر الرقمية.	30	3	5	3.71	0.84
يتم الحد من محاولا- الاختراق أو الاحتيال عبر المنصة الرقمية	30	3	5	3.68	0.86
يتم الشعور بوجود اجراءات تنظيمية واضحة تحكم استخدام الخدمات الإلكترونية	30	3	5	3.74	0.82
يتم احترام خصوصية البيانات الشخصية عند استخدام الخدمات الرقمية.	30	3	5	4.02	0.74
يتم طلب البيانات الضرورية فقط لإتمام المعاملات.	30	3,00	5,00	3.96	0.79
يتم حماية المعلومات الشخصية من الوصول غير المصرح به.	30	3	5	3.88	0.81
يتم الشعور بالأمان عند إدخال المعلومات الحساسة (مثل بيانات الهوية أو الدفع(	30	3	5	3.72	0.87
يتم عدم مشاركة البيانات الشخصية مع أطراف أخرى دون موافقة.	30	3	5	3.81	0.85
يتم توضيح سياسة حماية البيانات بشكل مفهوم للزبائن.	30	2	5	3.59	0.90
يتم الحفاظ على سرية المعاملات الإلكترونية المنجزة عبر المنصة	30	3,00	5,00	3.91	0.78
يتم تعزيز الثقة في المؤسسة نتيجة التزامها بحماية البيانات	30	3	5	4.05	0.73
يتم تعزيز الثقة في خدمات المؤسسة نتيجة توفر الأمن السيبراني.	30	3	5	4.08	0.72
يتم تفضيل التعامل. المؤسسة بسبب مستوى لأمان الرقمي المتوفر	30	3	5	3.84	0.82
يتم الشعور بالاطمئنان عند إجراء المعاملات الإلكترونية.	30	3	5	3.97	0.77
يتم تعزيز الرغبة في . . الاستمرار في التعامل مع المؤسسة بسبب حماية البيانات،	30	3,00	5,00	3.89	0.80
يتم التوصية بخدمات المؤسسة للآخرين نتيجة الثقة في أمنها الرقمي	30	3,44	4,88	3.76	0.86
يتم اعتبار الأمن السياني عاملاً مؤثرا في قرار اختيار المؤسسة	30	3	5	3.93	0.79
يتم تعزيز للمؤسسة في السوق بفضل التزاما بالأمن الرقمي	30	2	5	4.01	0.75
يتم الإحساس بأن حماية البيانات تمنح المؤسسة ميزة تنافسية مقارنة بالمؤسسات الأخرى	30	3	5	3.95	0.78

ملخص

تتناول هذه الدراسة "فعالية الأمن السيبراني في حماية بيانات العملاء"، مستهدفةً الكشف عن الدور الاستراتيجي الذي تلعبه أنظمة الحماية الرقمية في تعزيز ثقة العملاء وضمان سلامة معاملاتهم في ظل التحول الرقمي المتسارع. اعتمدت الدراسة على المنهج الوصفي التحليلي من خلال شقين؛ أحدهما نظري تناول مفاهيم الأمن السيبراني وعلاقته بالتسويق الخدماتي، والآخر ميداني طبق على عينة من العملاء باستخدام الاستبيان كأداة لجمع البيانات، بهدف قياس مدى تأثير فعالية الأمن السيبراني على الميزة التنافسية والسمعة التسويقية للمؤسسة.

وقد خلصت الدراسة إلى أن الأمن السيبراني لم يعد مجرد إجراء تقني فحسب، بل أصبح عاملاً استراتيجياً جوهرياً يؤثر بشكل مباشر على ولاء العملاء واستقطابهم. كما أثبتت النتائج وجود علاقة ذات دلالة إحصائية بين فعالية تدابير حماية البيانات وبين مستوى الثقة الممنوح للمؤسسة، مما يفرض على المؤسسات ضرورة الاستثمار المستمر في الأمن السيبراني وتبني سياسات حوكمة قوية لضمان مرونة أدائها التشغيلي وحماية خصوصية عملائها في البيئة الرقمية التنافسية.

الكلمات المفتاحية :الأمن السيبراني، بيانات العملاء، التحول الرقمي، ثقة العملاء، الميزة التنافسية، حوكمة الخصوصية.

Abstract

This study addresses the topic of "The Effectiveness of Cybersecurity in Protecting Customer Data," aiming to reveal the strategic role that digital protection systems play in enhancing customer trust and ensuring the integrity of their transactions in light of rapid digital transformation. The study adopted a descriptive analytical approach through two parts: a theoretical section covering cybersecurity concepts and its relationship with service marketing, and a field study conducted on a sample of customers using a questionnaire as the primary data collection tool. The objective was to measure the impact of cybersecurity effectiveness on the institution's competitive advantage and marketing reputation.

The study concluded that cybersecurity is no longer merely a technical measure but has become a fundamental strategic factor that directly impacts customer loyalty and acquisition. The results confirmed a statistically significant relationship between the effectiveness of data protection measures and the level of trust granted to the institution, which necessitates that organizations continuously invest in cybersecurity and adopt strong governance policies to ensure operational resilience and protect customer privacy in a competitive digital environment.

Keywords: Cybersecurity, Customer Data, Digital Transformation, Customer Trust, Competitive Advantage, Privacy Governance.