

دراسة تحليلية لخصوصية وأمن المعلومات المصرفية في بيئة البنوك الرقمية؛ دراسة حالة بنك بنكسي الجزائر. An Analytical Study on the Privacy and Security of Banking Information in a Digital Banking Environment: A Case Study of Bank Banxy Algeria

زيدان سمية¹ ، عصماني سفيان² / Zidane Soumia¹ , Osmani Sofiane²

¹ مخبر الدراسات والبحوث التسويقية والاقتصادية؛ جامعة سطيف 01؛ فرحات عباس ، soumia.zidane@univ-setif.dz

² مخبر الشراكة والاستثمار في المؤسسات الصغيرة والمتوسطة في الفضاء الأورومغاربي؛ جامعة سطيف 01؛ فرحات عباس

osmanisofiane@univ-setif.dz

تاريخ النشر: 2024/12/ 20

تاريخ القبول: 2024/12/ 12

تاريخ الاستلام: 2024/10/ 14

ملخص:

تتناول هذه الدراسة موضوع البنوك الرقمية والتي تقدم خدمات مالية مبتكرة تعتمد بشكل أساسي على تكنولوجيا المعلومات والاتصالات، حيث تم استعراض سياسة الخصوصية وكذلك الإجراءات الأمنية المتبعة من طرف بنك بنكسي، وقد توصلت الدراسة إلى أن بنك بنكسي يتبع سياسة خصوصية تتفق مع القوانين واللوائح الجزائرية والعالمية كما يعتمد على إجراءات أمنية متقدمة لمواجهة مختلف التهديدات السيبرانية

كلمات مفتاحية: خصوصية؛ أمن معلومات مصرفية؛ بنوك رقمية.

تصنيف JEL: G201, K220, K420.

Abstract:

This study addresses the topic of digital banking, which offers innovative financial services primarily based on information and communication technology. The study also reviews the privacy policy and security measures implemented by Bank Banxy. The study found that Bank Banxy follows a privacy policy that complies with Algerian and international laws and regulations and relies on advanced security measures to counter various cyber threats.

Keywords: Privacy; Banking information security; Digital Banks.

Jel Classification Codes: K420, K220, G201.

Résumé:

Cette étude aborde le sujet des banques numériques qui offrent des services financiers innovants reposant principalement sur les technologies de l'information et de la communication. L'étude examine également la politique de confidentialité et les mesures de sécurité mises en place par la Banque Banxy. L'étude conclut que la Banque Banxy suit une politique de confidentialité conforme aux lois et réglementations algériennes et internationales, et qu'elle repose sur des mesures de sécurité avancées pour faire face aux diverses menaces cybernétiques.

Mots-clés: confidentialité; sécurité des informations bancaires; banques numériques.

Codes de classification de Jel: K420, K220, G201.

المؤلف المرسل: عصماني سفيان، الإيميل: osmanisofiane@univ-setif.dz

1. مقدمة:

تعتبر البنوك الرقمية من أبرز الابتكارات في قطاع الخدمات المصرفية، حيث توفر تجربة مصرفية سهلة ومريحة للعملاء. ومع تزايد استخدام التكنولوجيا وتطورها، أصبحت خصوصية وأمن المعلومات المصرفية أمرا حائزا على أهمية كبيرة، حيث تواجه البنوك الرقمية العديد من التحديات في مجال خصوصية وأمن المعلومات، فعلى الرغم من التقدم التكنولوجي الذي يسهل إتاحة الخدمات المصرفية عبر الإنترنت والهواتف الذكية، إلا أن هناك تهديدات متعددة تهدد خصوصية وأمن المعلومات في هذا النوع من البنوك، مثل الاختراق الإلكتروني وسرقة الهوية والاحتيال المصرفي. وعلى هذا الأساس يتوجب على البنوك الرقمية أن تبذل قصارى جهدها لتوفير نظام أمن قوي يحمي بيانات العملاء ويضمن سرية معلوماتهم المصرفية.

1.1 إشكالية البحث: على ضوء ما سبق يمكن أن نطرح الإشكالية من خلال التساؤل الرئيسي:

ما مدى توافر سياسة خصوصية واضحة وإجراءات أمنية صارمة في مجال المعلومات المصرفية لدى بنك بنكسي؟

تندرج تحت إشكالية البحث التساؤلات التالية:

✓ ما المقصود بالبنوك الرقمية؟

✓ ما المقصود بسياسة الخصوصية؟

✓ ما المقصود بأمن المعلومات المصرفية؟

ما هي الإجراءات المعتمدة من طرف بنك بنكسي في مجال خصوصية وأمن المعلومات المصرفية؟

2.1 فرضيات البحث: يمكن صياغة فرضية رئيسية للبحث ممثلة فيما يلي

إن اعتماد بنك بنكسي على سياسة خصوصية واضحة وإجراءات قوية لأمن المعلومات هو الذي يساعده في أن يكون

البنك الرقمي الأول عبر الهاتف المحمول في الجزائر.

3.1 أهداف البحث: تتنوع الأهداف المرجو تحقيقها من وراء هذا البحث والذي يعتبر كمحاولة استطلاعية عن ظاهرة جديدة

في ميدان التكنولوجيا المالية ألا وهو سياسة و أمن المعلومات المصرفية كرافعة أساسية لتحقيق التحول الرقمي في مجال الخدمات المصرفية من خلال:

✓ يسعى البحث إلى إضافة معرفية لموضوعات التحول الرقمي بكونه يعالج موضوع البنوك الرقمية كأحد روافد التكنولوجيا المالية؛

✓ يسعى البحث كذلك إلى التأصيل المفاهيمي لموضوع البنوك الرقمية كمنفذ تكنولوجي حديث في تقديم الخدمات المصرفية الالكترونية؛

✓ يسعى البحث إلى توضيح مفهوم سياسة الخصوصية لدى البنوك الرقمية

✓ يسعى البحث إلى تسليط الضوء على الإجراءات اللازمة لأمن المعلومات المصرفية وسريتها في بيئة البنوك الرقمية

4.1 أهمية البحث: تكمن أهمية هذه الدراسة في كونها تركز على مناقشة متغيرات معاصرة ومستجدة في ظل البيئة الرقمية

والتي أصبحت تشكل أكبر التحديات التي تواجه البنوك، فالتغيرات الديناميكية في بيئات الأعمال نتيجة العولمة والتغير التكنولوجي ودخول التسويق غمار مرحلة الجيل الخامس الأمر الذي عجل بميلاد البنوك الرقمية أو كما تسمى بالبنوك الافتراضية والتي تعتبر كتقنية مبتكرة وملائمة للعديد من الأشخاص الذين يفضلون الوصول إلى خدمات البنوك بطريقة سهلة ومريحة في أي وقت ومكان، كما تكمن أهمية الدراسة كونها تلقي الضوء على قضية مهمة إذ تناقش سياسة الخصوصية بالإضافة إلى أمن المعلومات وسريتها ومحاولة الربط بينها وبين تبني الخدمات المصرفية الالكترونية وتزداد أهميتها من أهمية التحول الرقمي للبنوك في عصر الألفية الثالثة، وما تواجهه من مخاطر سيبرانية متعددة.

5.1 منهجية البحث: نظرا لطبيعة الموضوع والمتمثل في تحليل ممارسات أمن المعلومات المصرفية كمطلب لتبني خدمات البنوك الخلوية في ظل التحول الرقمي تم الاستناد على المنهج الوصفي من خلال الاستعانة بالكتب والمجلات العلمية المتخصصة بالإضافة إلى دراسة حالة المطبقة على بنك بنكسي.

2. مفهوم البنوك الرقمية: في ظل التطورات المتسارعة التي يشهدها العالم على صعيد التقنية والتكنولوجيا الحديثة والتي أدت إلى دخول الإنسانية إلى العصر الرقمي، برزت في الوجود وعلى الصعيد المالي ظاهرة جديدة نتيجة تطورات العصر الجديد، حيث ظهر ما يسمى بالبنوك الرقمية كأحد أبرز الابتكارات التي غيرت بشكل جذري طريقة تقديم الخدمات المالية والمصرفية حيث تشكل هذه البنوك مركزا للابتكار والريادة في القطاع المالي والتي تعتمد بشكل أساسي على التكنولوجيا الحديثة والقنوات الإلكترونية لتقديم خدماتها.

1.2 تعريف البنوك الرقمية: تشير البنوك الرقمية إلى توفير الخدمات المالية والأنشطة المصرفية من خلال القنوات الإلكترونية، وذلك بشكل أساسي باستخدام الإنترنت وتطبيقات الهاتف المحمول. وهذا يترتب عليه تقديم خدمات مصرفية متنوعة مثل إدارة الحسابات وتحويل الأموال ودفع الفواتير وطلبات القروض وإدارة الاستثمارات وغيرها وهذا دون الحاجة إلى الفروع المادية للبنوك التقليدية (Verma A, 2022, p. 16). كما تم تعريف البنوك الرقمية على أنها: المصارف الرقمية الجديدة، أو كما تُسمى أحيانا النيوبنك (Neobank)، هي عبارة عن جهات تقدم خدمات مالية تشبه الخدمات المصرفية التقليدية، ولكنها تعمل من خلال الانترنت أو تطبيقات الهاتف المحمول وتستهدف جذب فئات مختلفة من العملاء من خلال تصميم مبتكرات وميزات جديدة، وبغض النظر عن تطور هذه المصارف الرقمية الجديدة والتي ستصبح الوحيدة في السوق المالية في السنوات القادمة وهذا راجع إلى كونها تمتلك القدرة على التأثير على النموذج المصرفي التقليدي بشكل كبير (Bradford, 2020, p. 01).

انطلاقا مما سبق يمكننا القول أن البنوك الرقمية هي ناتج حصيلة التحول الرقمي الذي حصل على القطاع المالي مما أدى في نهاية المطاف إلى إتاحة تقديم الخدمات المصرفية التقليدية عبر قنوات إلكترونية ورقمية مثل الانترنت أو عن طريق تطبيقات الهواتف المحمولة، وتعتبر سهولة الوصول وكذلك سرعة المعاملات بالإضافة إلى القدرة العالية على تخصيص الخدمات المالية المصرفية وفق حاجات كل زبون من بين أهم الميزات التي تميز البنوك الرقمية عن التقليدية، وصفوة القول يمكن أن نشير إلى أن البنوك الرقمية تمثل تطورا هاما في صناعة الخدمات المالية من خلال تقديم تجربة مصرفية مبتكرة ومرنة تلي تطلعات العملاء في العصر الرقمي.

2.2 أهمية البنوك الرقمية: تعتبر البنوك الرقمية الوجه الأمثل للتحول الرقمي وعلى هذا الأساس تبرز أهمية هذا النوع من البنوك كونها تستجيب لتطلعات العملاء في العصر الرقمي ويمكن توضيح أهمية البنوك الرقمية في العصر الرقمي من خلال النقاط التالية (Vijayashree, 2022, pp. 273-274):

1.2.2 الراحة (Convenience): يمثل هذا العنصر النقطة المركزية التي تؤدي للعملاء إلى تبني هذا النوع من الخدمات المصرفية الرقمية، حيث يتيح عنصر الراحة للعملاء وللمستخدمين إدارة أمورهم المالية في أي وقت ومن أي مكان، من خلال هواتفهم الذكية أو أجهزتهم الحاسوبية ودون الرجوع إلى الفروع البنكية التقليدية.

2.2.2 سهولة الاستخدام (Ease of Use): يشير مصطلح سهولة الاستخدام إلى مدى قدرة العملاء على الاستفادة من الخدمات المصرفية الإلكترونية دون مواجهة صعوبات أو تعقيدات، ويشمل هذا المفهوم جوانب مختلفة مثل البساطة والوضوح وإمكانية الوصول وسهولة الاستعمال، حيث يقوم البنك الرقمي بتبسيط العمليات من خلال واجهات سهلة

زيدان سمية، عصماني سفيان ،: دراسة تحليلية لخصوصية وأمن المعلومات المصرفية في بيئة البنوك الرقمية؛ دراسة حالة بنك بنكسي الجزائر
الاستخدام والتشغيل الآلي مما يجعل المهام مثل دفع الفواتير، وتحويل الأموال، ومراقبة الحسابات سهلة للغاية، لذلك
يعكس مفهوم سهولة الاستخدام في جوهره فعالية التصميم والوظيفة في تسهيل تفاعل المستخدم وتحقيق النتائج المرجوة
بأقل جهد أو إحباط.

3.2.2 فعالية التكلفة (Cost-effectiveness): تعمل الخدمات المصرفية عبر البنوك الرقمية على تقليل تكلفة الوصول إلى
الخدمات المالية بشكل كبير، سواء بالنسبة للأفراد أو المؤسسات المالية. فإذا كانت الخدمات المصرفية التقليدية تتضمن
تكاليف عامة مرتبطة بالمحافظة على الفروع المادية والموظفين والبنية التحتية، في حين أن الخدمات المصرفية عبر الهاتف
المحمول تعمل على التخلص من هذه التكاليف، مما يسمح للمؤسسات المالية بتقديم الخدمات بتكلفة أقل للعملاء، ويترجم
هذا الانخفاض في التكاليف إلى انخفاض الرسوم والتكاليف مما يجعل الخدمات المالية ميسورة التكلفة ومتاحة لقطاع
أوسع من السكان.

4.2.2 تعزيز الأمن والثقة (Enhancing Security and trust): حققت منصات الخدمات المصرفية عبر الهاتف المحمول
تطورات كبيرة في ضمان أمن المعاملات المالية. حيث نفذت البنوك والمؤسسات المالية تدابير أمنية قوية، مثل التشفير
والمصادقة متعددة العوامل والتحقق البيومتري لحماية بيانات المستخدم ومنع الوصول غير المصرح به. وقد ساهمت هذه
الميزات الأمنية إلى جانب سهولة الخدمات المصرفية عبر الهاتف المحمول في غرس الثقة لدى العملاء وشجعتهم على اعتماد
الخدمات المصرفية عبر الهاتف المحمول كوسيلة آمنة وموثوقة لإدارة شؤونهم المالية.

5.2.2 تجربة العملاء والتخصيص (Customer experience and personnalisation): تركز تطبيقات الخدمات المصرفية
المقدمة عبر البنوك الرقمية بشكل متزايد على تعزيز تجربة العملاء من خلال التعديل (Customisation) أو
التخصيص (Personalisation) وذلك من خلال الاستفادة المتزايدة من برمجيات الذكاء الاصطناعي وكل ذلك من أجل
تقديم تجارب شخصية ومصممة خصيصاً لعملائها انطلاقاً من تحليل سلوك العملاء الإلكتروني.

3.2 العوامل المؤثرة في نية استخدام البنوك الرقمية: يتأثر استخدام البنوك الرقمية من قبل العملاء بمجموعة من
العوامل التقنية والتي تعمل مجتمعة على تسهيل تقبل واستخدام هذا النوع من الخدمات والتي نوضحها في النقاط التالية:

1.3.2 الموثوقية (Reliability): وتعني القدرة على الالتزام بالخدمات المقدمة بطريقة تمكن المستخدم من الاعتماد عليها
باستمرارية وبدقة عالية، وتحقيق الوعود التي التزم بها البنك بتقديم الخدمات المصرفية الإلكترونية بشكل متكامل تلي
متطلبات الزبائن، كما أنها مؤشر مهم لقياس الجودة في قطاع البنوك الرقمية يجب تقديم كل خدمة بطريقة مثلى لأن
الفشل في تقديم الخدمات يقود إلى تدمير العملاء (Erlane K. Ghan, 2022, p. 05).

2.3.2 الخصوصية (Privacy): تشير إلى قدرة البنك في المحافظة على البيانات والمعلومات الشخصية لزبائنه، واستحالة
الكشف عن البيانات المرسلة أو المخزنة لدى البنك، فهو عامل مهم يعمل على توفير فرصة للبنوك الرقمية لبناء علاقة
جيدة مع عملائه من خلال فهم تصوراتهم مثل العادات الشرائية، تفاصيل المعلومات عن حساباتهم، حجم المعاملات،
حركات الحساب والكثير من البيانات التي تعكس خصوصية الزبائن (Juan-Gabriel Martínez-Navalón, 2023, p. 785).

3.3.2 سهولة التصفح (navigation of Ease): وتعني القدرة على التنقل في استخدام تطبيقات البنك الرقمي بكل سهولة
وهذا ما يؤثر على مستوى رضا الزبائن مما يزيد الموثوقية والولاء لديهم في استخدام التطبيق وهذا ما يتطلب بعض
الخصائص وهي اللغة المستخدمة ووضوح محتوى المعلومات.

4.3.2 الأمن (Security): ويعني توفير الثقة وهي أهم العوامل التي تساعد على استخدام واستمرار خدمة البنك الرقمي،
والحماية التي يوفرها البنك ضد تهديدات الأمن والسيطرة على المعلومات الشخصية المرسلة من وإلى البنك عند استخدام
التطبيق، كما تعني مدى تصور الزبائن من الحماية التي يوفرها البنك ضد تهديدات الأمن والسيطرة على المعلومات
الشخصية المرسلة من وإلى البنك عند استخدام خدمات البنوك الرقمية وبذلك يعتبر عنصر الأمن الدعامات الأساسية
لوجود واستمرارية تقديم الخدمات المصرفية الإلكترونية وبدونه ينتفي هذا النوع من الخدمات (Juan-Gabriel Martínez-Navalón, 2023, p. 785).

5.3.2 التعقيد (Complexity): أدت التطورات المتسارعة على أصعدة تحرير وعولمة الخدمات المالية وتكنولوجيا المعلومات المصرفية إلى تنوع نشاطات البنوك وتعقيد البنية التحتية التكنولوجية لها، ولكن درجة التعقيد يجب أن تكون على نحو محدد في الخدمة المقدمة لكي لا يجد العميل صعوبة في الفهم واستخدام النظام.

3. الخصوصية في بيئة البنوك الرقمية: تمثل المعلومات عصب المنظمات وأساس أدائها لمهامها في العصر الرقمي، فنوع المعلومات وكميتها وطريقة عرضها تشكل حجر الأساس لنجاح صنع القرارات داخلها. ولذلك، تُصبح المعلومات ذات قيمة عالية تستوجب وضع ضوابط صارمة لتنظيم استخدامها وتداولها، وضمان حيازتها بشكل سليم. ومن هنا تأتي الحاجة إلى توفير حماية قوية للمعلومات وحمايتها من الاستخدام غير المشروع. وعلى هذا الأساس ارتبط مفهوم الخصوصية المعلوماتية ارتباطاً وثيقاً بالخشية من مخاطر جمع ومعالجة بيانات الأفراد لأغراض غير معلنة أو غير مشروعة، أو إساءة استخدامها أو تحويلها إلى جهات أخرى دون موافقتهم. كما تركز على حقوق أصحاب البيانات ومدى سيطرتهم عليها.

1.3 مفهوم خصوصية المعلومات المصرفية: بشكل عام يمكن التعبير على مفهوم الخصوصية على أنه قدرة الفرد أو الجماعة على التحكم في الوصول إلى معلوماتهم الشخصية ونشرها، كما تتضمن الخصوصية الحق في الحفاظ على سرية جوانب معينة من حياة الفرد أو معلوماته الشخصية، واتخاذ قرارات مستقلة حول كيفية وموعد ومع من يتم مشاركة المعلومات، بالإضافة إلى ذلك تشمل الخصوصية أبعاداً مختلفة، بما في ذلك الخصوصية الشخصية والمعلوماتية، وتلعب دوراً جوهرياً في الحفاظ على الاستقلالية والكرامة والحرية في كل من السياقات المادية والرقمية. وقد تم تقديم العديد من التعريفات لمفهوم خصوصية المعلومات المصرفية، حيث وفي هذا الصدد تم تعريف مفهوم الخصوصية على أنها: خصوصية المعلومات تشير إلى قدرة الأفراد أو المنظمات على التحكم في جمع واستخدام ونشر معلوماتهم الشخصية (Piotrowski, 2023, p. 123). وهذا يعني ضمان التعامل مع البيانات الحساسة، مثل المعلومات الشخصية والبيانات المالية والسجلات الصحية وأي معلومات خاصة أخرى، بطريقة تحترم حقوق الأفراد وتحافظ على السرية، وبذلك تعد الخصوصية جانباً أساسياً للحفاظ على الثقة والأمن في بيئة الأعمال الإلكترونية. كما تم تعريف الخصوصية كذلك على أنها: الخصوصية هي الحق القانوني الذي يتمتع به الفرد في التحكم المعلومات المتعلقة به وتحديد كيفية مشاركتها مع الآخرين (Aggelos Kiayias, 2022, p. 1743)، وبذلك تشكل هذه الخصوصية أساس القواعد التي تحكم جمع وإدارة البيانات الشخصية كمعلومات بطاقة الهوية والمعلومات المالية والسجلات الطبية والرسائل والمكالمات الهاتفية وغيرها من جملة البيانات والمعلومات، وعلى هذا الأساس ترتبط خصوصية المعلومات ارتباطاً وثيقاً بمفهوم حماية المعلومات.

انطلاقاً مما سبق يمكن القول أن مفهوم الخصوصية المعلوماتية والتي يشار إليها كذلك بخصوصية البيانات أو حماية البيانات، هي عبارة عن قدرة الأفراد أو المنظمات على التحكم في معلوماتهم الشخصية والتي لا يمكن مشاركتها إلى أطراف أخرى إلا من خلال موافقتهم على ذلك، ومن هذا المنطلق تعتبر الخصوصية المعلوماتية مفهوماً أساسياً في عالمنا الرقمي الحالي، حيث تمنح الأفراد القدرة على السيطرة على معلوماتهم الشخصية وتعزيز الثقة في التفاعلات الإلكترونية والتي نذكر على وجه الخصوص منها الخدمات المالية لما لها من حساسية متزايدة لدى الأفراد والمنظمات.

2.3 أدوات الحماية التقنية لخصوصية المعلومات في البنوك الرقمية: على الرغم من المخاوف الكثيرة التي يطرحها موضوع الخصوصية في بيئة البنوك الرقمية إلا أنه وبفضل التطورات التقنية الحديثة، بات بإمكان البنوك والعملاء من استخدام برامج ووسائل جديدة توفر الحماية والأمان لخصوصيتهم، سواء كانت برامج أمنية مخصصة للمستخدم العادي أو البنوك الرقمية، أو برامج أمنية للشبكات تخدم البنوك الرقمية بصفة خاصة، بالإضافة إلى تقنيات التشفير باختلاف أنواعها ومن بين أهم الأدوات التقنية لحماية الخصوصية نذكر على سبيل المثال لا الحصر الأدوات التالية:

زيدان سمية، عصماني سفيان ،: دراسة تحليلية لخصوصية وأمن المعلومات المصرفية في بيئة البنوك الرقمية؛ دراسة حالة بنك بنكسي الجزائر

1.2.3 بروتوكول تفضيلات الخصوصية(P3P): هذا البرنامج أو البروتوكول تم تطويره من طرف الجمعية العالمية للشبكة العالمية(World Wide Web Consortium) ويهدف هذا النوع من البرامج لتوفير المزيد من التحكم للمستخدمين من ضبط تفضيلات خصوصيتهم على المتصفحات التي يعملون عليها ومن ثم زيادة تعزيز الخصوصية لهم على الانترنت الأمر الذي يؤدي إلى حماية المعلومات الشخصية لهم مما يساهم بشكل كبير للعملاء في التعامل مع البنوك الرقمية دون هواجس (Robert W. Reeder, 2008, p. 11).

2.2.3 برامج إخفاء الهوية(Anonymity software): يتم استعمال هذا النوع من البرامج لتأمين تصفح الانترنت عن طريق خادم وكيل(Server) والذي يعمل بدوره كأداة لحظر أو حذف أو إدارة ملفات تعريف الارتباط(الكوكيز)، الأمر الذي يؤدي إلى حماية خصوصية المستخدمين عبر الإنترنت من خلال إخفاء هوياتهم على الإنترنت، مثل عناوين(IP) وتاريخ التصفح والنشاط على الإنترنت، مما يجعل من الصعب على المواقع الإلكترونية والمعلنين تتبع المستخدمين وجمع بياناتهم الشخصية، وفي مجال البنوك الرقمية فإن هذا النوع من البرامج يوفر الحرية للعملاء عند التعامل معها بشكل سري وأمن من عمليات التلصص والتتبع (Brazier, 2004, p. 138).

3.2.3 نظام بي جي بي (Pretty Good Privacy/PGP): يعتبر هذا النوع من الأنظمة أو البرامج الأكثر موثوقية على الإطلاق كونه يوفر طبقة حماية قوية للمستخدمين من خلال توفير مفهوم الخصوصية التشفيرية(التشفير المتماثل والتشفير ذو المفتاح العام) بالإضافة إلى المصادقة على تبادل البيانات مما يعزز من الحفاظ على سريتها بالإضافة من التحقق من هوية المرسل وبالتالي تعزيز مفهوم الخصوصية والأمان وهذا ما تسعى إليه البنوك الرقمية في نهاية المطاف (Alexander Yakubov, 2020, p. 4).

3.3 المبادئ العالمية لحماية الخصوصية في البنوك الرقمية: أقر المجلس الأمريكي والكندي مجموعة من القواعد الأساسية التي يتوجب على المنظمات أخذها بعين الاعتبار في العصر الرقمي، وباعتبار البنوك الرقمية منظمات تعمل على الخط مباشرة ففي هذه الحالة هي ملزمة أكثر من أي وقت مضى للالتزام بهذه المبادئ والتي نذكرها في النقاط التالية (Auditors, 2009, p. 7):

1.3.3 الإدارة(Management): يلتزم البنك بتطبيق مجموعة من الإجراءات والسياسات الهادفة لحماية خصوصية المعلومات الشخصية التي يكون بصدد جمعها، مع تحديد الأشخاص المسؤولين عن عملية الجمع وإخضاعهم للمساءلة في حالة تم تسريب أو التلاعب بهذه المعلومات خارج الإطار المحدد لها.

2.3.3 الإشعار(Notice): يلتزم البنك بتقديم إشعارا حول سياسات وإجراءات الخصوصية الخاصة به مع تحديد الأغراض التي يتم من أجلها جمع المعلومات الشخصية حول العملاء مع توضيح طريقة استخدامها وكيفية الاحتفاظ بها وضرورة الإفصاح عنها كلما دعت الحاجة إلى ذلك.

3.3.3 الخيار والموافقة(Choice&Consent): يتعين على البنك توضيح الخيارات المتاحة للأفراد ومن ثم تحصل على موافقة صريحة فيما يتعلق بجمع واستخدام معلوماتهم الشخصية مع ضرورة الإفصاح عنها وقت الضرورة، مما يعني أن البنك لا يمكنه في أي حال من الأحوال جمع معلومات شخصية ما لم يوافق العملاء على ذلك بصراحة.

4.3.3 الجمع(Collection): يلتزم البنك فقط بجمع المعلومات الشخصية لتحقيق الأغراض المحددة في إشعار سياسة الخصوصية الخاصة به.

5.3.3 الاستعمال، الاحتفاظ والتخلص(Use, Retention&Disposal): يلتزم البنك باستخدام المعلومات الشخصية لعملائه وفقا للأغراض المحددة سلفا في إشعار الخصوصية الخاصة به والتي تمت الموافقة الصريحة عليها من قبل العملاء، كما يلتزم البنك بالاحتفاظ بهذه المعلومات ضمن مدة زمنية محددة حسب ما تقتضيه اللوائح أو النصوص القانونية المسيرة لسياسات الخصوصية وبعد الانتهاء من الاستخدام يتم التخلص منها بطريقة سليمة ومناسبة.

6.3.3 الوصول(Access): يلتزم البنك بتوفير عنصر الإتاحة لعملائه من خلال الوصول إلى معلوماتهم الشخصية من أجل إجراء عملية المراجعة والتصحيح وكذلك القيام بعملية التحديث.

7.3.3 الإفصاح عن المعلومات لأطراف ثالثة (Disclosure to Third parties): يتعين على البنك الكشف عن المعلومات الشخصية لعملائه إلى أطراف خارجية أو كما يطلق عليها الأطراف الثالثة فقط وفق الأغراض المحددة في إشعار سياسة الخصوصية الخاصة به وبموافقة ضمنية أو صريحة من طرف العملاء وبطريقة توفر حماية مماثلة لتلك المعلومات.

8.3.3 أمن الخصوصية (Security for Privacy): يتعين على البنك باتخاذ إجراءات معقولة لحماية المعلومات الشخصية لعملائه الشخصية من فقدان أو الوصول غير المصرح به.

9.3.3 الجودة (Quality): يلتزم البنك بالمحافظة على المعلومات الشخصية ذات الصلة، الدقيقة والكاملة وفق الأغراض المحددة في إشعار سياسة الخصوصية مع التعهد على صون سلامة هذه المعلومات.

10.3.3 المراقبة والتنفيذ (Monitoring & Enforcement): يتوجب على البنك مراقبة مدى الامتثال لسياسات وإجراءات الخصوصية الخاصة به؛ مع ضرورة توفير الإجراءات السارية لمعالجة الشكاوي والنزاعات المتعلقة بالخصوصية.

4. أمن المعلومات المصرفية في بيئة البنوك الرقمية: يعتبر أمن المعلومات المصرفية أمراً ذا أهمية كبيرة في عالم البنوك الرقمية، لذلك فإن الحفاظ على أمن المعلومات المصرفية للعملاء يعزز الثقة في الخدمات المصرفية الرقمية ويحفي المعلومات الشخصية للعملاء من الوصول غير المصرح به. بالإضافة إلى ذلك يمكن ضمان سرية المعلومات المصرفية للعملاء من القيام بمعاملاتهم المالية بأمان وثقة، مما يساهم في تعزيز التجربة المصرفية الإلكترونية والرقمية.

1.4 مفهوم أمن المعلومات المصرفية: : يعتبر أمن المعلومات المصرفية الركيزة الأساسية كي تستطيع البنوك الرقمية من مواصلة نشاطها وفي هذا الصدد تم تعريف أمن المعلومات المصرفية على أنه: يشير أمن المعلومات المصرفي إلى كل الممارسات والتقنيات المستخدمة لحماية أي بيانات أو معلومات مرتبطة بعمليات البنوك الرقمية والتي من ضمنها معلومات العملاء وتفاصيل الحساب (الأرصدة، المعاملات) أو أي وثائق رقمية مثل الكشوفات والفواتير وغيرها (Solange Ghernaouti, 2005, p. 140)، ويمكن الهدف من أمن المعلومات المصرفية في البنوك الرقمية إلى تحقيق مفهوم السرية والتي تعني ان الوصول إلى البيانات المالية الحساسة لا يكون إلا للأشخاص المخولين بذلك بالإضافة إلى تحقيق مفهوم النزاهة والتي تشير إلى أن المعلومات تظل دقيقة وغير متغيرة طوال دورة حياتها. كما تم تعريف أمن المعلومات المصرفية على أنها: يمثل أمن المعلومات المصرفية (BIS) نظاماً متكاملًا لحماية البيانات المالية الحساسة على مدار دورة حياتها، حيث يعتمد هذا النظام على تطبيق نهج يجمع بين الضوابط الفنية والضمانات الإدارية وإجراءات التحكم بالوصول، حيث يهدف هذا النظام يهدف إلى حماية سرية وسلامة المعلومات المالية، بالإضافة إلى التقليل من المخاطر المتعلقة بالهجمات الإلكترونية واختراق البيانات والوصول غير المصرح به وكل ذلك من أجل ضمان السير السلس للبنوك الرقمية وتحقيق ثقة العملاء (Alfredo Leonidas Vasquez Ubalo, 2023, p. 98).

انطلاقاً مما سبق يمكن القول أن أمن المعلومات المصرفية هو مجموعة من السياسات والممارسات والتقنيات التي تهدف إلى حماية المعلومات المالية والشخصية للعملاء، كما يشمل أمن المعلومات المصرفية الحماية من الاختراقات الإلكترونية وسرقة البيانات المالية بالإضافة إلى ضمان سلامة التحويلات المصرفية والتأكد من هوية العملاء وحمايتهم. وصفوة القول يمكن أن نقول أن أمن المعلومات المصرفية يعد عنصراً أساسياً لتبني خدمات البنوك الرقمية وهذا من خلال استخدام تقنيات متقدمة لضمان الحفاظ على الخصوصية والسرية للمعلومات المصرفية.

2.4 خدمات الأمن الأساسية للعمليات المصرفية في البنوك الرقمية: تعتبر خدمات الأمن للعمليات المصرفية أمراً ضرورياً لحماية البيانات والممتلكات المالية للعملاء وركيزة أساسية لضمان استمرارية العمليات المصرفية في البنوك الرقمية، وعلى هذا الأساس تعد خدمات الأمن للعمليات المصرفية جزءاً أساسياً من أي بنك رقمي ناجح. وفي هذا الخصوص يمكن القول

زيدان سمية، عصماني سفيان ،: دراسة تحليلية لخصوصية وأمن المعلومات المصرفية في بيئة البنوك الرقمية؛ دراسة حالة بنك بنكسي الجزائر
أنه توجد خمسة أنواع أساسية لخدمات الأمن للمعلومات المصرفية في البنوك الرقمية والتي نوضحها في النقاط التالية (LI)
:FANG, 2023, pp. 57-59)

1.2.4 خدمات حماية التعريف (Identification and Authentication): تهدف هذه الخدمات إلى التأكد من هوية الشخص بشكل دقيق، لاسيما عند تقديم معلومات تعريفية للبنك الرقمي، وذلك من خلال التحقق من صحة هذه المعلومات وضمان تطابقها مع هوية الشخص الفعلية.

2.2.4 خدمات السيطرة على الدخول (Access Control): تستخدم هذه الخدمات بمثابة درع واق ضد الدخول غير المصرح به إلى مصادر الأنظمة والاتصالات والمعلومات الخاصة بالبنك الرقمي، ولذلك تعد خدمات التحكم بالدخول بوابات أساسية للتحقق من هوية المستخدمين ومنحهم الصلاحيات المناسبة.

3.2.4 خدمات السرية (Confidentiality): تقدم هذه الخدمات حلولاً فعالة لمنع تسريب المعلومات المصرفية إلى جهات غير مصرح لها بالحصول عليها. ويتم تحقيق ذلك من خلال تطبيق مبدأ السرية والذي يعرف على أنه إخفاء المعلومات عن طريق تشفيرها.

4.2.4 خدمات حماية التكاملية وسلامة المحتوى (Data and message Integrity): تقدم هذه الخدمات حلولاً فعالة لحماية البيانات من التغيير غير المتعمد أو المتعمد خلال دورة حياتها. وتساهم هذه الخدمات أيضاً في حماية البيانات من الإتلاف الكامل أو الإلغاء غير المصرح به.

5.2.4 خدمات منع الإنكار (Non-repudiation): تلعب هذه الخدمات دوراً هاماً في ضمان عدم قدرة أي جهة على إنكار مسؤوليتها عن نقل البيانات أو تنفيذ أي نشاط مُحدد.

3.4 تقنيات أمن المعلومات في البنوك الرقمية: تواجه الخدمات المالية عبر البنوك الرقمية تحديات كبيرة تتعلق بحساسية البيانات والأمان، مما يثير قلقاً وخوفاً لدى العملاء قد يعيق إقبالهم على هذه الخدمات. لذلك تلجأ البنوك الرقمية إلى مجموعة من الإجراءات التقنية والتي تهدف إلى حماية أنظمتها من جهة وتعزيز شعور العملاء بالأمان من جهة أخرى ومن بين هذه الإجراءات التقنية نذكر ما يلي:

1.3.4 تقنيات التحقق والوصول الآمن (Secure Authentication and Access techniques): يمكن تعريف تقنيات المصادقة والوصول الآمنة على أنها هي الطرق المستخدمة للتحقق من هوية المستخدمين ومنحهم الإذن بالوصول إلى نظام أو مورد معين مع الحفاظ على سلامة وسرية البيانات، وعلى هذا الأساس تعد تقنيات التحقق والوصول الآمن مكونات أساسية لأي نظام بما فيها البنوك الرقمية، وفي هذا الصدد هناك طريقتان وهما (N. A. Karim, 2024, p. 745):

1.1.3.4 المصادقة ذات العامل الواحد (Single-factor Authentication): يعتمد هذا النوع من المصادقة على عامل واحد من الأدلة لإثبات هوية المستخدم، وعادة ما يكون اسم المستخدم وكلمة المرور.

2.1.3.4 المصادقة متعددة العوامل (Multi-factor Authentication): يطلب هذا النوع من المصادقة من المستخدمين تقديم عاملين أو أكثر للتحقق من هويتهم للحصول على الصلاحية للوصول إلى النظام، ويمكن أن تشمل هذه العوامل شيئاً يعرفه المستخدم فقط (مثل كلمة المرور)، أو شيئاً يملكه المستخدم فقط (مثل الرمز المميز أو البطاقة الذكية)، أو شيئاً يميز المستخدم بيولوجياً (مثل بصمة الإصبع أو التعرف على الوجه).

2.3.4 تقنيات الحماية من الاختراقات والاحتيال (Hacking and Fraud Protection techniques): تعد تقنيات الحماية من الاختراقات والاحتيال ضرورية لحماية بيانات وأنظمة البنوك الرقمية من الوصول غير المصرح به ومن الخسائر المالية، حيث تشمل على مجموعة من الإجراءات والتقنيات التي تهدف إلى منع الهجمات الالكترونية والتصدي لأنشطة الاحتيال. فيما يلي شرح لبعض الطرق الرئيسية (Alhuseen O. Alsayed, 2017, pp. 110-113):

1.2.3.4 جدران الحماية (Firewalls): هي أنظمة أمنية للشبكات تراقب وتتحكم في حركة المرور الواردة والصادرة عبر الشبكة، حيث تعمل كحاجز بين جهاز الكمبيوتر أو الشبكة الخاصة بالبنوك الرقمية والفضاء السيبراني، والهدف الأساسي منها محاولات الوصول غير المصرح بها وتمنع دخول البرامج الضارة إلى نظام البنوك الرقمية.

2.2.3.4 تقنيات كشف الاختراق (Intrusion Detection Techniques): تعني تقنيات كشف الاختراق الأساليب والتقنيات المستخدمة لتحديد والاستجابة للأنشطة غير المصرح بها أو الخبيثة داخل شبكة الكمبيوتر أو النظام للبنوك الرقمية، حيث تتضمن هذه التقنيات مراقبة حركة الشبكة وسجلات النظام ومصادر البيانات الأخرى لاكتشاف السلوك المشبوه أو علامات اختراق أمني محتملة، لذلك فتقنيات كشف الاختراق تشبه حراس الأمن الرقمي الذين يراقبون نظام أو شبكة البنوك الرقمية باستمرار للبحث عن الأنشطة المشبوهة، فهي تساعد في تحديد ومنع محتمل محاولات الوصول غير المصرح بها، وانتهاكات النظام، وغيرها من الأفعال الخبيثة.

3.2.3.4 تقنيات كشف الاحتيال (Fraud Detection techniques): تعتبر تقنيات كشف الاحتيال أداة أساسية للمؤسسات المالية بما فيها البنوك الرقمية والأفراد على حد سواء، وهذا لمكافحة الخسائر المالية والأنشطة الاحتيالية، لذلك يمكن القول أن تقنيات كشف الاحتيال هي جملة الأساليب والاستراتيجيات المستخدمة لتحديد ومنع وتخفيف الأنشطة الاحتيالية داخل البنوك الرقمية، حيث تتضمن هذه التقنيات تحليل مصادر بيانات وأنماط وسلوكيات مختلفة للكشف عن الشذوذ أو علامات الاحتيال المحتمل، ويبقى الهدف من هذه التقنيات هو الكشف عن السلوك الاحتيالي ومنع الخسائر المالية وحماية الأصول والحفاظ على سلامة الأنظمة والعمليات لدى البنوك الرقمية.

3.3.4 تقنيات التشفير والتوقيع الرقمي (Encryption and digital signature techniques): يعتبر كل من التشفير والتوقيع الرقمي عمودين أساسيين في الأمن السيبراني للبنوك الرقمية، حيث يعملان معا لضمان سرية البيانات وسلامتها وأصالتها، لذلك تعد كل من تقنيات التشفير والتوقيع الرقمي مكونات أساسية لأمن المعلومات لدى البنوك الرقمية حيث تُستخدم لحماية سرية البيانات وسلامتها ومصداقيتها كما يلي (Farid Lalem, 2023, pp. 4-5):

1.3.34 تشفير البيانات (Data encryption): تشتمل تقنيات التشفير على ترميز البيانات بطريقة لا يمكن فك تشفيرها إلا من قبل الأطراف المصرح لها والذين يمتلكون مفتاح فك التشفير المناسب، مما يعمل على بقاء المعلومات الحساسة سرية وأمنة أثناء النقل أو التخزين.

2.3.34 التوقيع الرقمي (Digital signature): تتضمن تقنيات التوقيع الرقمي استخدام خوارزميات التشفير لإنشاء توقيع رقمي فريد لمقطوعة بيانات أو وثيقة، حيث يعمل هذا التوقيع على التحقق من صحة وسلامة البيانات مما يضمن عدم العبث بها وأنها صادرة عن المرسل المتوقع.

5. دراسة تفصيلية لمفهوم الخصوصية وأمن المعلومات المصرفية لدى بنك بنكسي الجزائر

1.5 نبذة عن بنك بنكسي (Banxy) المحمول: هو أول بنك نقال في الجزائر، أطلقته شركة ناتكسيس الجزائر (Natixis Algérie) والمنتمية للمجموعة المصرفية (BPCE) وكان ذلك بتاريخ 23 أبريل 2018 واسمه بنك بنكسي (Banxy Bank)، حيث عمل مصرف ناتكسيس على استغلال ازدهار سوق الهواتف المحمولة وفرص الرقمنة في السوق المصرفي الجزائري مما أدى في نهاية الأمر إلى ابتكار نوعا جديدا من الخدمات المصرفية الالكترونية في السوق الجزائرية. يقدم بنك بنكسي خدمات جديدة تسعى لتسهيل الحياة اليومية للجزائريين. حيث يمكنهم من فتح حساب مؤمن، ويمكن الولوج إليه عن طريق هاتف

زيدان سمية، عصماني سفيان ، : دراسة تحليلية لخصوصية وأمن المعلومات المصرفية في بيئة البنوك الرقمية؛ دراسة حالة بنك بنكسي الجزائر
ذكي، في أي وقت وفي أي مكان، أي أنه عبارة عن خدمات بنكية عن بعد وفي متناول الجميع وبدون الحاجة إلى التنقل إلى مقر البنك المادي.

وقد حقق التطبيق نجاحًا كبيرًا، حيث تم تحميله أكثر من 500000 مرة من متجر (Google Play Store). كوما
صف (Banxy) بأنه ثالث أفضل تطبيق في فئة التطبيقات المالية المجانية بناءً على تقييمات المستخدمين. كما تحصل بنك
بنكسي جائزة أفضل بنك رقمي من مجلة (Global Finance) عام 2021 وجائزة أفضل ابتكار في الخدمات المصرفية من
مجلة (The Banker) عام 2022، وجائزة أفضل تجربة عميل من مجلة (Euromoney) عام 2023، وكل هذه الجوائز إنما
تعبر بشكل دقيق وأكد على مدى تفرد وتميز بنك بنكسي في مجال الخدمات المصرفية الالكترونية (Banxy Natixis 2024
(Algérie).

2.5 خطوات التسجيل في تطبيق بنك بنكسي: يلتزم بنك بنكسي بتوفير تجربة سهلة ومثيرة ومتميزة من أجل مواكبة
التكنولوجيا المالية وهذا من خلال اتباع مجموعة من الخطوات والتي نوجزها فيما يلي (Banxy N. , comment-ouvrir-un
:compte, 2024)

1.2.5 تحميل تطبيق بنكسي (سهل ومجاني): للاكتتاب في بنكسي، ما على الزبون سوى تحميل التطبيق من أحد برامج
التحميل (App Store)، أو (Play Google)، ثم إنشاء وترسيم حسابه. والشكل رقم 1 يوضح مراحل فتح حساب بنكي في
بنكسي .

2.2.5 شروط اشتراك بسيطة: يمكن لأي شخص بلغ سن الرشد ملء استمارة التسجيل من التطبيق، ثم إدخال رقم هاتفه
وعنوان بريده الإلكتروني المستعمل
3.2.5 يقوم البنك بالتحقق من الوثائق اللازمة لفتح الحساب من خلال عقد مقابلة فيديو آمن يديره أحد مكلف الزبائن
بالبنك.

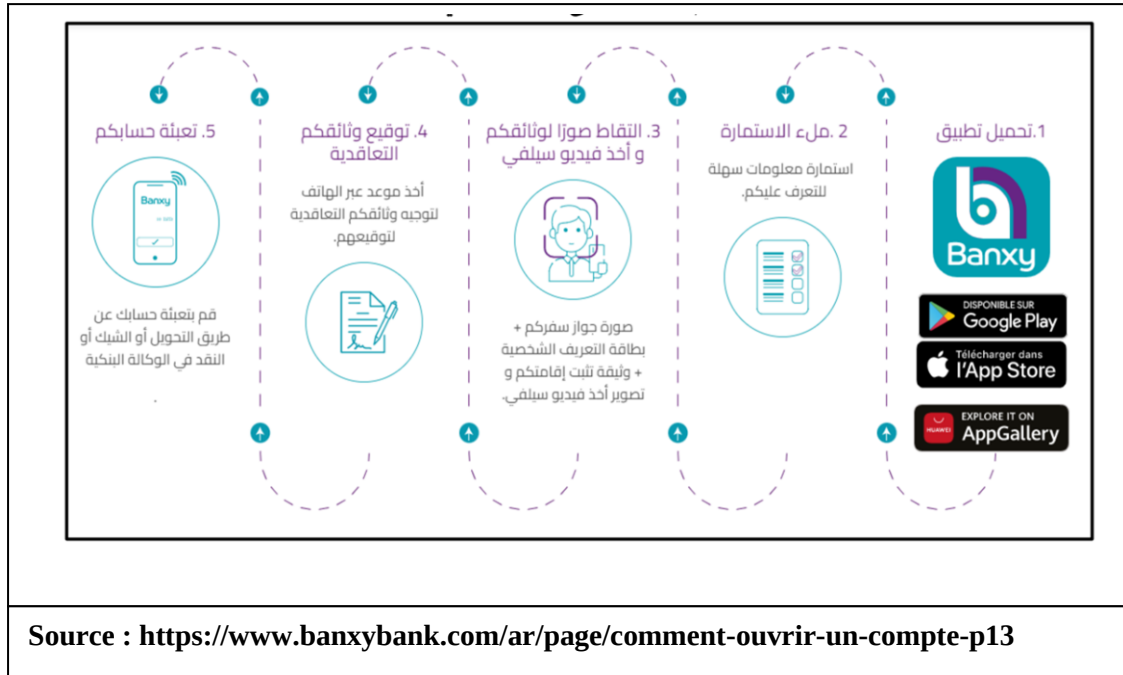
4.2.5 لإتمام فتح الحساب، سيتم تسليم المستندات القانونية مباشرة إلى الزبون في مقر سكنه أو أي مكان يختاره لجمع
توقيعه بخط اليد. يتم تنشيط الحساب بعد استلام والتحقق من الملف الفعلي من قبل البنك. كما يوفر البنك بنكسي مركز
علاقات الزبائن على مدار 12 ساعة في اليوم، حتى في أيام السبت، لتقديم أي مساعدة مطلوبة.

5.2.5 بمجرد فتح حساب بنكسي، يقوم المستخدمون بالاتصال بشكل آمن مزود بمعلومات البنك الموجود في الجزائر، وذلك
بفضل اسم المستخدم وكلمة السر الخاصة بهم.

6.2.5 وكأخر مرحلة يتم تكوين كلمة سرية فائقة (PIN) بواسطة الزبون للتحقق من صحة كل معاملة من معاملاته. كما
لدى بنكسي نظام كامل لحماية بيانات الزبائن وفقا لأعلى المعايير الدولية، وتستخدم أحدث تكنولوجيا ونظام الحلول
الحسابية لضمان أمن زبائنها وبياناتهم.

والشكل الموالي يوضح وبطريقة بسيطة وسهلة كيفية فتح حساب لدى بنك بنكسي المحمول كما يلي:

الشكل رقم(01): مراحل فتح حساب بنكسي



3.5 خصوصية المعلومات في بنك بنكسي: يستخدم بنك بنكسي تطبيقاته لجمع البيانات عبر الإنترنت لتقديم مجموعة متنوعة من الخدمات لعملائه، من إدارة الحسابات إلى المعاملات المالية حيث تخضع هذه التطبيقات أيضا لسياسات خصوصية تحدد كيفية جمع البيانات واستخدامها ومشاركتها، حيث يلتزم بنك بنكسي بمعالجة البيانات الشخصية وفقا للقانون الجزائري رقم(07-18) المتعلق بحماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية، وهذا القانون مماثل تقريبا للتشريعات الأوروبية لحماية البيانات العامة (GDPR).

1.3.5 سياسية الخصوصية لدى بنك بنكسي: امتثالا للقانون الجزائري رقم(07-18) المتعلق بحماية وخصوصية المعلومات، تم إنشاء سياسة الخصوصية للمهتمين بكيفية استخدام المعلومات المحددة للهوية الشخصية عبر الإنترنت، حيث يتعلق الأمر بمعلومات يمكن استخدامها بمفردها أو مع معلومات أخرى لتحديد هوية شخص ما أو الاتصال به أو تحديد موقعه بمفرده أو في سياقه المحيط، كما تم وضع سياسة لخصوصية المعلومات في بنك بنكسي لكي يكون هناك فهم واضح لكيفية جمع، استخدام، وحماية المعلومات المحددة للهوية الشخصية الخاصة بالعملاء على جميع منصاته الإلكترونية: الموقع الإلكتروني والتطبيق (بنكسي) على (Android و iOS) والتصرف فيها.

1.1.3.5 ملفات الارتباط وحماية الخصوصية: يهتم بنك بنكسي بخصوصية عملائه أثناء تصفحهم لموقعه الإلكتروني أو تطبيقه المعتمد، كما يتيح البنك لعملائه التحكم في كيفية استخدام ملفات تعريف الارتباط على أجهزتهم (مثل أجهزة الكمبيوتر، الهواتف الذكية، الأجهزة اللوحية، الخ.) من خلال خيارات قابلة للتعديل في أي وقت، وسيتم شرح كيفية عمل ملفات تعريف الارتباط وكيفية ضبط إعدادات متصفحات العملاء للتحكم الأمثل بها، (Natixis B. , gestion-des-cookies, 2023).

أ. ملفات تعريف الارتباط الأساسية لاستعمال الموقع: يتعلق الأمر بملفات تعريف ارتباط يتم وضعها من طرف بنك بنكسي على جهاز العملاء من أجل متطلبات التصفح والأداء الأمثل على موقعه. والجدول الموالي يوضح ذلك:

زيدان سمية، عصماني سفيان ، : دراسة تحليلية لخصوصية وأمن المعلومات المصرفية في بيئة البنوك الرقمية؛ دراسة حالة بنك بنكسي الجزائر
الجدول رقم(01): ملفات تعريف الارتباط الأساسية لموقع بنك بنكسي

الوظيفة	اسم ملف تعريف الارتباط
مُعرف الجلسة	_ci_sense
اختيار اللغة	user_lang
Source : https://www.banxybank.com/ar/page/gestion-des-cookies-p185	

ب. ملفات تعريف الارتباط الموجهة لقياس الإقبال: يتم وضع هذا النوع من ملفات تعريف الارتباط لأغراض إحصائية وتحليلية، حيث يقوم بنكسي وبشكل خاص بتتبع عدد الصفحات التي تم زيارتها، وعدد الزيارات، بالإضافة إلى نشاط المتصفحين على الموقع وتكرار زيارتهم، ويعود ذلك بفضل استخدام حلول قوغل أناليتيكس (Google Analytics). والجدول الموالي يوضح ذلك:

الجدول رقم(02): ملفات تعريف الاحصائية لموقع بنك بنكسي

الوظيفة	اسم ملف تعريف الارتباط
قياس الإقبال	gat_gtag_UA_140392065_1_
قياس الإقبال	gid_
معرّف الجلسة	ga_
Source : https://www.banxybank.com/ar/page/gestion-des-cookies-p185	

ج. ملفات تعريف الارتباط الخاصة بالطرف الثالث (Third-Party Cookies) : هذا النوع من ملفات تعريف الارتباط يتم وضعه من قبل جهات خارجية مثل شركات الخدمات أو الشركاء، حيث يتم استخدامها بشكل شائع لتتبع سلوك العملاء عبر الإنترنت عبر مواقع ويب متعددة. على سبيل المثال قد تحتوي صفحة الويب لبنك بنكسي على عناصر مخزنة على خوادم نطاقات أخرى (مثل الصور أو المحتوى المضمن مثل مقاطع الفيديو من (YouTube)، أو العروض التقديمية من (Flickr)، وما إلى ذلك و على هذا الأساس يمكن أن تقوم هذه المواقع بتعيين ملفات تعريف الارتباط الخاصة بها عند استرجاع المكونات الخارجية خلال التصفح (Banxy N. , 2024).

ويهدف بنك بنكسي من خلال ملفات تعريف الارتباط إلى تحقيق جملة من الأهداف التي تعمل على تحقيق فهم احتياجات العملاء بشكل عميق والعمل على تخصيص الخدمات لهم بشكل يحقق تقديم الخدمات المصرفية الالكترونية بشكل يحقق الرضا لدى العملاء ويمكن توضيح باقي الأهداف من وراء استعمال بنك بنكسي لملفات تعريف الارتباط في النقاط التالية (Banxy N. , 2024) :

- ✓ مساعدة بنك بنكسي في فهم تفضيلات عملائه بناءا على سلوكهم السابق أو الحالي على الموقع، مما يسمح بتقديم خدمة أفضل؛
 - ✓ مساعدة بنك بنكسي في جمع بيانات شاملة حول معدلات زيارة الموقع وتفاعلاته، مما يسمح بتحسين تجربة العملاء على الموقع في المستقبل؛
 - ✓ تجميع بيانات حول معدلات زيارة الموقع وتفاعلات العملاء معه لتوفير تجارب وأدوات أفضل على الموقع في المستقبل؛
 - ✓ يمكن للمتجر أيضا استخدام خدمات موثوقة تابعة لجهات خارجية لتتبع هذه المعلومات نيابة عنه.
- كما يتيح بنك بنكسي لعملائه خيارات للتحكم بملفات تعريف الارتباط، تتراوح من تلقي إشعار عند وضع كل ملف تعريف ارتباط إلى حظر جميع ملفات تعريف الارتباط، حيث يتم ذلك من خلال إعدادات المتصفح والتي تختلف من

متصفح لآخر، و لمعرفة كيفية تعديل إعدادات ملفات تعريف الارتباط، ينصح بالعملاء إلى الرجوع إلى خيار المساعدة في القائمة العلوية للمتصفح لتطبيق بنك بنكسي.

2.3.5 حماية المعلومات لدى بنك بنكسي لتحقيق مفهوم الخصوصية: يعتبر مفهوم حماية البيانات الجانب الحاسم في الخدمات المصرفية الرقمية، حيث تضمن مبدأ الأمان والخصوصية للمعلومات المالية والشخصية للعملاء. كما يلتزم بنك بنكسي بخصوص المعلومات الشخصية للعملاء، حيث لا يقوم بنك بنكسي ببيع أو تبادل أو تحويل معلومات عملائه إلى أطراف ثالثة دون الحصول على موافقة صريحة من المستخدم، ويستثنى من ذلك الشركاء الذين يساعدون البنك في تشغيل موقعه الإلكتروني وتقديم خدمة العملاء وهذا بشرط التزامهم بالحفاظ على سرية هذه المعلومات، كما قد يضطر بنك بنكسي إلى الكشف على معلومات في بعض الحالات الاستثنائية وهذا امتثالا للقانون أو القواعد المنظمة بالإضافة إلى حماية حقوق العملاء أو حقوق الغير أو لحماية الممتلكات أو لحماية الأمن. كما يمكن لبنك بنكسي مشاركة معلومات عامة وغير حساسة غير مرتبطة بهوية العملاء مع أطراف ثالثة لأغراض التسويق أو الإعلان أو غيرها. وصفوة القول يمكن القول أن بنك بنكسي يضطلع بكل مسؤولية على حماية المعلومات الخاصة للعملاء كما يلتزم بأوامر القانون الجزائري المحدد لحماية المعلومات وتحقيق الخصوصية بدرجة عالية.

4.5 أمن المعلومات لدى البنك الخلوي بنكسي: نظرا لكونه المبتكر لهذا النوع من الخدمات على مستوى الجزائر والسباق الأول (The Pioneer) في إنشاء أول بنك خلوي ونظرا لحساسية هذا النوع من الخدمات كونها تحمل مخاطر ثنائية؛ حيث تتعلق الأولى بالمخاطرة المالية التي قد يتعرض لها العملاء وتتعلق الثانية بمخاطر السمعة التي قد تصيب البنك في مقتل من خلال فشل البنك في تعزيز تسويق هذا النوع من الخدمات المالية الجديدة نظير التخوف الذي يبديه المستهلكون والعملاء تجاه هذا النوع من الخدمات، لذلك يولي بنك بنكسي على عاتقه اهتماما ومسؤولية كبيرتين بأمن المعلومات وهذا من خلال إدراكه لأهمية حماية بيانات العملاء الشخصية والمالية، ولتحقيق ذلك فإن بنك بنكسي يستخدم مجموعة من التقنيات والإجراءات المتقدمة لضمان سلامة وأمان البيانات والمعلومات والتي نوجزها في النقاط التالية:

1.4.5 تقنيات الحماية لدى بنك بنكسي: يلتزم بنك بنكسي بصفة دائمة ومستمرة بتطبيق التقنيات الحديثة في مجال أمن المعلومات المصرفية وهذا نظرا لحساسية هذه المعلومات من جهة، وإلى السعي إلى تحقيق مبدأ الثقة والأمان لدى عملائه مما يسمح بتبني هذا النوع من الخدمات ومن ثم تحقيق مفهوم الشمول المالي ويمكن توضيح أهم التقنيات التي يعتمد عليها بنك بنكسي في هذا المجال في النقاط التالية:

1.1.4.5 تشفير البيانات (Data Encryption): يستخدم بنك بنكسي أحدث التقنيات المتواجدة في مجال التشفير وهذا يخص جميع البيانات الحساسة بما في ذلك أرقام حسابات العملاء وكلمات المرور الخاصة بهم وهذا تفاديا لأي طارئ قد يحدث في المجال السيبراني من تسلل من قبل الهاكرز أو دخول غير مصرح به من طرف أشخاص في حالة فقدان جهاز الهاتف المحمول لعمل البنك بالإضافة إلى حماية بيانات البنك وعملائه من أي تجسس يضره بالدرجة الأولى وعملاؤه بالدرجة الثانية؛ وفيما يلي أهم تقنيات التشفير المعتمدة من طرف البنك (Natixis B., encryption, 2024):

أ. التشفير المتماثل (Symmetric encryption): الهدف من هذا النوع من التشفير هو السماح لبنك بنكسي للوصول الحصري فقط لبيانات عملائه حيث يتم استخدام هذا النوع من التشفير لتشفير وفك التشفير للبيانات باستخدام نفس المفتاح والذي يعرف باسم المفتاح السري والذي يكون حسب الخطوات التالية:

- ✓ وضع المفتاح السري بعد تحويل البيانات إلى نص مشفر؛
- ✓ يتم إرسال النص المشفر إلى الطرف (المستقبل)؛
- ✓ تتم عملية فك تشفير النص المشفر من قبل الطرف المستقبل من خلال استعمال نفس المفتاح السري.

ب. التشفير غير المتماثل (Asymmetric encryption): يختلف هذا النوع من التشفير عن سابقه كونه يتم عن طريق استعمال مفتاحين، المفتاح العام والذي يستخدم لتشفير البيانات والمفتاح الخاص الذي يستخدم لفك تشفير البيانات، وتكمن أهمية هذا النوع من التشفير في كونه مؤمن إلى أبعد الحدود ففي حالة وصول أي شخص إلى المفتاح العام فإنه لا يستطيع الوصول إلى المفتاح الخاص والذي يكون حصرا عند بنك بنكسي؛ ومن بين أهم استعمالات هذا النوع من التشفير هو إنشاء توقعات رقمية للتحقق من صحة المعاملات ومنع الاحتيال؛

ج. التشفير باستخدام التجزئة (hash-based encryption): هذا النوع من التشفير جد متقدم كونه يعتمد على إنشاء بصمة رقمية فريدة للبيانات لا يمكن تقليدها أو تزويرها والهدف من وراء ذلك هو تحقيق أكبر قدر من التحقق على سلامة البيانات وبالتالي الحرص على عدم تغييرها، وهذا ما يبرز أهمية هذا النوع من التشفير كونه يتميز بالأمان والكفاءة والنزاهة، ويمكن توضيح طريقة عمل هذا النوع من التشفير في النقاط التالية:

- ✓ يقوم بنك بنكسي بإدخال البيانات إلى دالة التجزئة؛
- ✓ تعمل دالة التجزئة بحساب قيمة ثابتة للبيانات المدخلة؛
- ✓ بما عملية التجزئة هي أحادية الاتجاه فإن عملية استعادة البيانات غير ممكنة وهذا ما يعزز قوة أمان هذا النوع من التشفير للبيانات.

2.1.4.5 جدران الحماية (Firewall): من أجل حماية الشبكة بشكل دوري ولمواكبة التهديدات التي الأمنية التي قد تطرأ في الفضاء السبيرياني فإن بنك بنكسي يستخدم جدران حماية متعدد الطبقات وهذا من أجل حماية شبكته من الوصول غير المصرح به، وفي هذا الصدد فإن البنك يعتمد بشكل أساسي على ثلاثة أنواع من الجدران كما يلي (Natixis B. , Firewall, 2024):

أ. جدار حماية داخلي (Internal Firewall) : وتتمثل المهمة الأساسية لجدار الحماية الداخلي إلى منع ورصد الوصول غير المصرح به داخل الشبكة الداخلية لبنك بنكسي بالإضافة إلى التحقق من هوية المستخدمين لدى بنك بنكسي؛

ب. جدار حماية خارجي (External Firewall): وتتمثل المهمة الأساسية لجدار الحماية الخارجي في كونه جهاز أمان شبكة بنك بنكسي حيث يراقب ويحكم حركة المرور بين الشبكة الداخلية لبنك بنكسي وبين الشبكة الخارجية وبعبارة أخرى فإن هذا النوع من الجدران مكلف بشكل أساسي على منع الوصول غير المصرح به إلى الشبكة الداخلية للبنك وحمايتها من الهجمات الضارة؛

ج. جدار حماية التطبيقات (Application Firewall): يعتبر هذا النوع من الجدران بمثابة الدرع الواقي الذي يعتمد عليه بنك بنكسي لحماية تطبيقاته من الهجمات الضارة مثل حقن (SQL) واختراق المواقع (XSS) وتزييف طلبات المواقع (CSFR)، كما يعتبر هذا النوع من الجدران كونه ضمانا وتأكيدا صارما على أن بنك بنكسي ملتزم بشكل صريح بالقوانين واللوائح المتعلقة بحماية البيانات مما يوفر عنصر الثقة بين البنك وعملائه، بالإضافة إلى كونه برنامج حماية فإن هذا النوع من الجدران يمتد إلى وظيفة أخرى تسويقية والتي تتمثل في تحسين تجربة المستخدم (User Experience).

3.1.4.5 أنظمة الكشف عن الاختراق (Intrusion Detection Systems - IDS): تعتبر أنظمة الكشف عن الاختراق جزءا مهما من تكنولوجيا أمان المعلومات المصرفية لدى بنك بنكسي، وهي بمثابة أنظمة أمان شبكية مصممة للكشف على الأنشطة المشبوهة على الشبكة من خلال فحص حركة مرور الشبكة وتحليلها بدقة للكشف عن أي أنماط تدل على أنشطة ضارة قد تهدد أمن البنك وبعدها يقوم بإرسال تنبيهات إلى مسؤولي الأمن للبنك حتى يتمكنوا من اتخاذ الإجراءات اللازمة لحماية البنك من أي تهديد ضار، ويمكن اعتبار هذا النوع من الأنظمة بمثابة جهاز أمن إستباقي (Natixis A. , 2024).

4.1.4.5 أنظمة منع الاختراق (Intrusion Prevention Systems - IPS): من أجل الوصول بالخدمات المصرفية الالكترونية إلى أرقى مكانتها في الجزائر وخاصة عبر الهاتف المحمول ومن أجل تعزيز وبناء الثقة لدى عملائه يعتمد بنك بنكسي على منظومة أمنية متقدمة تحصن أنظمتها وبياناته من أي مخاطر محتملة وهذا من خلال الاعتماد على أنظمة الكشف عن

الاختراق وصولاً إلى أنظمة منع الاختراق والتي تعمل على إبطال الهجمات الإلكترونية قبل وقوعها ونذكر هنا على سبيل الذكر لا الحصر نظام إدارة الأحداث والمعلومات الأمنية (Security Information and Event Management) (Natixis A. , 2024).

2.4.5 إجراءات الحماية لدى بنك بنكسي: يتبع بنك بنكسي بالإضافة إلى التقنيات الرقمية الحديثة مجموعة أخرى من الإجراءات التقنية والتي تهدف أساساً إلى تحقيق مستوى فاعل لأمن المعلومات المصرفية لديه يضيّاهي ويتوافق مع الإجراءات العالمية المعمول بها في هذا المجال والتي نذكرها في النقاط التالية (Banxy A. , 2024):

1.2.4.5 سياسة التحكم في الوصول (Access Control Policy): من أجل حماية بيانات العملاء وأنظمة البنك من الوصول غير المصرح به فإن بنك بنكسي يتبع سياسة تحكم في الوصول صارمة وقواعد مشددة والتي تهدف من ورائها إلى ضمان أن يتمتع العملاء فقط بإمكانية الوصول إلى حساباتهم ومعلوماتهم الشخصية بشكل آمن ومسؤول ومن أجل تحقيق هذه الغاية فإن بنك بنكسي يتبع الإجراءات التالية:

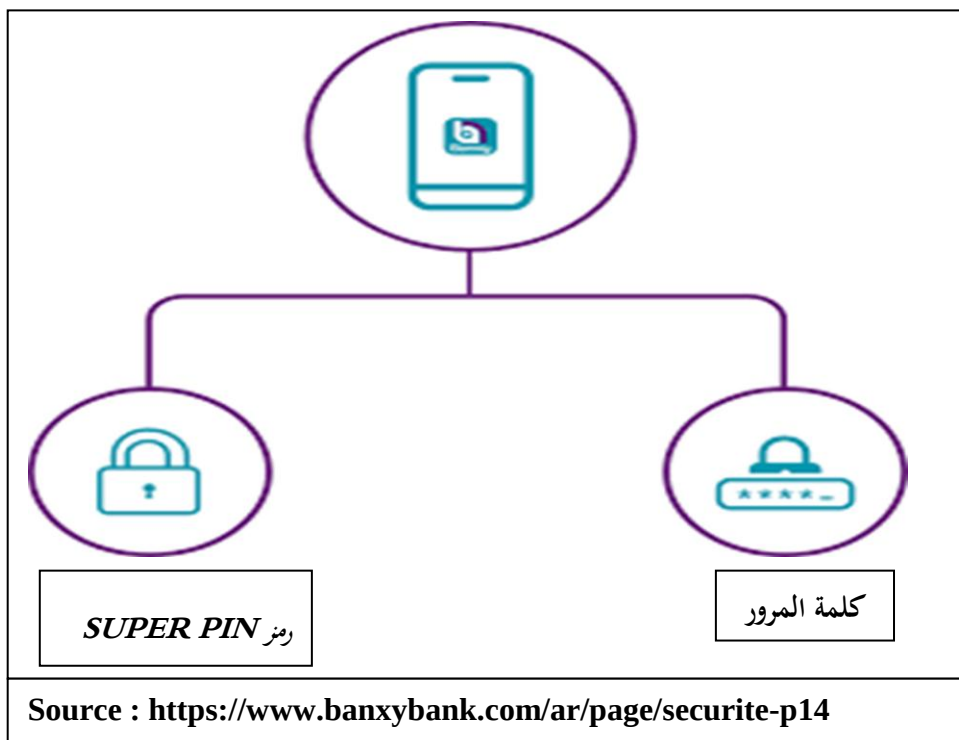
أ. التعريف (Authentication): يمكن اعتبار التعريف كإجراء وقائي لحماية بيانات العملاء وأنظمة البنك، حيث يطلب من جميع العملاء إثبات هويتهم ويمكن أن يتم ذلك من خلال مجموعة من إجراءات التعريف الموضحة في النقاط التالية:

✓ كلمات المرور؛

✓ بصمات الأصابع؛

✓ الأرقام السرية (PIN). والشكل الموالي يوضح ذلك:

الشكل رقم (02): إجراءات التعريف لدى بنك بنكسي



ب. التسجيل والمراجعة (Logging and Review): يتم تسجيل جميع عمليات الوصول إلى أنظمة بنك بنكسي وبيانات العملاء ويقوم بنك بنكسي بمراجعة هذه السجلات بشكل دوري ومنتظم للتأكد من عدم وجود أي نشاط غير عادي الأمر الذي يساعد بنك بنكسي على ضمان أمن بيانات العملاء وأنظمة البنك من أي تهديد خارجي.

زيدان سمية، عصماني سفيان ،: دراسة تحليلية لخصوصية وأمن المعلومات المصرفية في بيئة البنوك الرقمية؛ دراسة حالة بنك بنكسي الجزائر

2.2.4.5 سياسة أمن المعلومات (Information Security Policy): يتبع بنك بنكسي سياسة أمن معلومات صارمة والتي تعد من أهم الأولويات لدى البنك والتي يهدف من ورائها إلى حماية سرية المعلومات وكذلك سلامة أنظمة البنك من الخروقات أو التهديدات الخارجية بالإضافة إلى الوصول غير المصرح به ويعتمد في ذلك على مجموعة واسعة من التقنيات سألقة الذكر بالإضافة إلى تطبيقه لنظام (3D SECURE) وهو نظام يعزز أمن المدفوعات عبر الشبكة.

3.2.4.5 برامج التوعية والتدريب لدى الموظفين (Employee Awareness and Training Programs): نظرا لأهمية أمن المعلومات الالكترونية يولي بنك بنكسي اهتماما كبيرا ببرامج التوعية والتدريب لموظفيه وهذا قصد تحقيق لأكبر قدر في حماية بيانات العملاء وأنظمة البنك من أي مخاطر إلكترونية محتملة والهدف من وراء ذلك هو الوصول إلى تمكين الموظفين من التعرف على المخاطر الالكترونية وكيفية التعامل معها بالإضافة إلى تعليم الموظفين أفضل الممارسات الواجب إتباعها لحماية أمن البيانات وأنظمة البنك الأمر الذي يعزز ويرفع من مستوى وعي الموظفين في مجال أمن المعلومات الالكترونية.

بالإضافة إلى جملة التقنيات والإجراءات المتبعة من قبل بنكسي فإن هذا الخير يقوم بتوعية عملائه وتقديم النصائح إليهم في سبيل حماية أمن المعلومات الخاصة بهم والتي نوجزها في النقاط التالية:

- ✓ استخدام كلمة مرور قوية وفريدة من نوعها لكل حساب؛
- ✓ عدم مشاركة معلوماتهم الشخصية أو المالية مع أي شخص؛
- ✓ توخي الحذر من رسائل البريد الإلكتروني أو المكالمات الهاتفية المشبوهة؛
- ✓ التأكد من أن جهازهم محمي ببرنامج مكافحة الفيروسات وجدار الحماية؛
- ✓ تحديث تطبيق بنكسي بانتظام.

3.4.5 تقييم سياسة الخصوصية ومستوى أمن المعلومات لدى بنك بنكسي: انطلاقا من عرض سياسة الخصوصية لدى بنك بنكسي يتضح أن هذا الأخير يتبع سياسة خصوصية واضحة تمتثل بالأساس مع القوانين واللوائح الجزائرية المتعلقة بحماية وخصوصية المعلومات بالإضافة إلى ذلك فهي تتفق كذلك مع التشريعات العالمية (الأوروبية والأمريكية)، كما يلتزم بنك بنكسي في إظهار سياسة الخصوصية على موقعه عبر الانترنت وهو ما يتفق تماما مع موثيق هيئة تراسست الالكترونية (TrustE) المنظمة لمفهوم سياسة الخصوصية على المستوى العالمي. أما على مستوى أمن المعلومات المصرفية والذي يعد عنصرا أساسيا في ضمان اعتماد الخدمات المصرفية عبر الهاتف المحمول، فكلما زادت ثقة العملاء في أمان معلوماتهم المالية، زاد احتمال تبنيهم لهذه الخدمات، فإن بنك بنكسي يُولي أهمية كبيرة لأمن المعلومات وحماية بيانات عملائه من خلال إتباعه نهجاً شاملاً لأمن المعلومات، والذي يشمل كل من تقنيات التحقق (المصادقة) والوصول الآمن، بالإضافة إلى تقنيات الكشف عن الاختراق والاحتيال مع الاعتماد على تقنيات التشفير العالمية مضافا إليها برامج التوعية الأمنية لموظفيه وكذلك عملائه وهو الأمر الذي أهله لأن يكون البنك المحمول الأول في الجزائر وهو ما يؤكد صحة الفرضية الموضوعة.

6. خاتمة:

في ختام هذه الدراسة، يمكننا القول بأن تحليل سياسة الخصوصية وممارسات أمن المعلومات في البنوك الرقمية يمثل أمرا حيويا وضروريا في ظل التحول الرقمي الذي يشهده قطاع الخدمات المصرفية. من خلال دراسة حالة بنك بنكسي في الجزائر، تبين أن النجاح في تبني خدمات البنوك الخلوية يعتمد بشكل كبير على استراتيجيات الأمن التي تعتمدها البنوك الرقمية مع ضرورة توضيح سياسة الخصوصية للعملاء.

1.6 نتائج البحث:

- التحول الرقمي في ظل التطور التكنولوجي المتسارع يشكل للعصر الرقمي ضرورة حتمية لكل المنظمات بما فيها البنوك والمصارف إذا أرادت البقاء في سوق تنافسية ومتغيرة جوهرها الإبداع التكنولوجي في تقديم الخدمات المصرفية

- تعتبر خصوصية وأمن المعلومات المصرفية وحمايتها في ظل التحول الرقمي عنصرا ذو أهمية كبيرة لا تقل عن أهمية باقي عناصر المزيج التسويقي لبنك بنكسي؛
- يعتبر بنك بنكسي السباق والريادي في مجال تقديم الخدمات المصرفية الالكترونية عبر تطبيقات الهاتف المحمول؛
- أظهرت النتائج أن لدى بنك بنكسي سياسة خصوصية واضحة حول جمع المعلومات وتتفق مع اللوائح والقوانين الجزائرية والعالمية؛
- يحوز بنك بنكسي على سياسة أمن معلومات واضحة والمسؤولية وملخصة ومحددة، الأمر الذي مكنه من دخول سوق الخدمات المصرفية الالكترونية عبر الهاتف المحمول بثقة وحرية.
- أظهرت الدراسة أن بنك بنكسي يطبق العديد من ممارسات أمن المعلومات المصرفية، مثل التشفير، والمصادقة الثنائية، والمراقبة المستمرة، والتأمين ضد الاحتيال.
- ساعدت هذه الممارسات في تحسين مستوى الأمن في البنك، مما أدى إلى زيادة ثقة العملاء في خدمات بنكسي

2.6 مقترحات البحث:

- يجب على بنك بنكسي إجراء اختبارات الاختراق بشكل دوري لتحديد نقاط الضعف في تقنيات حماية الوصول. كما يمكن استخدام اختبارات الاختراق لتحسين تقنيات حماية الوصول ومنع الهجمات الإلكترونية؛
- يجب تحديث أنظمة الأمن السيبراني بشكل مستمر ومتواصل، وذلك لمواكبة التطورات التكنولوجية والتغيرات في الأمن السيبراني، وتعزيز قدرة المصرف على الوقاية من الهجمات السيبرانية والتعامل معها بشكل فعال؛
- العمل على مواكبة المعايير الدولية في مجال سياسة الخصوصية وكذلك أمن المعلومات المصرفية؛
- العمل على سلامة أنظمة وإجراءات تقنية المعلومات والحماية المتكاملة للبيانات من أجل الحصول على شهادة الإيزو(27001) لأمن المعلومات المصرفية مما يعزز ويرفع لها مستوى الثقة لدى عملائها.

7. المراجع:

1. Aggelos Kiayias, M. K. (2022). PEReDi: Privacy-Enhanced, Regulated and Distributed Central Bank Digital Currencies. *ACM SIGSAC Conference on Computer and Communications Security (CCS '22)*, (pp. 1739-1752). Los angels, USA.
2. Alexander Yakubov, W. S. (2020). BlockPGP: A Blockchain-based Framework for PGP Key Servers. *International Journal of Networking and Computing* , 10 (01), 1-24.
3. Alfredo Leonidas Vasquez Ubalo, a. Y. (2023). Information Security in the Banking Sector: A Systematic Literature Review on Curren Trends, Issues, and Challenge. *International Journal of Safety and Security Engineering* , 13 (01), 97-106.
4. Alhuseen O. Alsayed, A. L. (2017). E-Banking Security: Internet Hacking, Phishing Attacks, Analysis and Prevention of Fraudulent Activities. *International Journal of Emerging Technology and Advanced Engineering* , 07 (01), 109-115.
5. Auditors, T. I. (2009). *Generally Accepted Privacy Principles*. Canada: American Institute of Certified Public Accountants(AICPA)/(CICA).
6. Banxy, A. (2024). *procedures Security*. Retrieved April 10, 2024, from www.banxybank.com/ar/page/securite-p14
7. Banxy, N. (2024). *comment-ouvrir-un-compte*. Retrieved April 20, 2024, from www.banxybank.com/fr/page/comment-ouvrir-un-compte-p13

8. Banxy, N. (2024). *politique-de-confidentialite*. Retrieved may 10, 2024, from [www.banxybank.com](https://www.banxybank.com/ar/page/politique-de-confidentialite-p4): <https://www.banxybank.com/ar/page/politique-de-confidentialite-p4>
9. Bradford, T. (2020). *Neobanks: Banks by Any Other Name?* KANSAS CITY: FEDERAL RESERVE BANK OF KANSAS CITY.
10. Brazier, F. O. (2004). Anonymity and Software Agents: An Interdisciplinary Challenge. *Artificial Intelligence and Law* , 12 (01), 137-157.
11. Erlane K. Ghan, M. M. (2022). The Effect of Perceived Usefulness, Reliability, and COVID-19 Pandemic on Digital Banking Effectiveness: Analysis Using Technology Acceptance Model. *Sustainability* , 14 (11), 1-16.
12. Farid Lalem, A. L. (2023). A Novel Digital Signature Scheme for Advanced Asymmetric Encryption Techniques. *Applied Sciences* , 13 (01), 2-15.
13. Juan-Gabriel Martínez-Navalón, M. F.-F. (2023). Does privacy and ease of use influence user trust in digital banking applications in Spain and Portugal? *International Entrepreneurship and Management Journal* , 19 (1), 781-803.
14. LI FANG, D. G. (2023). Security Measures Applied on Digital Banking Towards Service Improvement Proposal. *Journal of Business and Management Studies* , 02 (01), 47-77.
15. N. A. Karim, O. A. (2024). Online Banking User Authentication Methods: A Systematic Literature Review. *IEEE Access* , 12 (01), 741-757.
16. Natixis, A. (2024). *Intrusion Detection Systems*. Retrieved April 09, 2024, from [/www.banxybank.com](https://www.banxybank.com/fr/recherche-articles?search=Intrusion+Detection+Systems): <https://www.banxybank.com/fr/recherche-articles?search=Intrusion+Detection+Systems>
17. Natixis, B. (2024). *encryption*. Retrieved february 12, 2024, from [www.banxybank.com](https://www.banxybank.com/ar/faq#faq_624): https://www.banxybank.com/ar/faq#faq_624
18. Natixis, B. (2024). *Firewall*. Retrieved April 13, 2024, from [www.banxybank.com](https://www.banxybank.com/ar/recherche?search=firewall): <https://www.banxybank.com/ar/recherche?search=firewall>
19. Natixis, B. (2023). *gestion-des-cookies*. Retrieved April 12, 2024, from [www.banxybank.com](https://www.banxybank.com/ar/page/gestion-des-cookies-p185): <https://www.banxybank.com/ar/page/gestion-des-cookies-p185>
20. Piotrowski, D. (2023). Privacy frontiers in customers' relations with banks. *Economics and business review* , 9 (01), 119-141.
21. Robert W. Reeder, P. G. (2008). A User Study of the Expandable Grid Applied to P3P Privacy Policy Visualization. *WPES'08: 7th ACM Workshop on Privacy in the Electronic Society*, (pp. 10-21). Alexandria, Virginia, USA.
22. Solange Ghernaouti, M. A. (2005). Guaranteering Security of Financial Transaction by Using Quantum Cryptography in Banking Environment. *the Second International Conference on E-Business and Telecommunication Networks* (pp. 139-149). United Kingdom: ICETE.
23. Verma A, M. S. (2022). Growth in Use of Banking in India. *Global Journal of Management and Sustainability* , 01 (01), 14-20.
24. Vijayashree, M. (2022). Recent Trends, Major Opportunities and Challenges of Digital Banking in Indian Context. *International Journal of Research Publication and Reviews* , 13 (10), 269-276.