جامعة قاصدي مرباح – ورقلة

كلية العلوم الاقتصادية والتجارية وعلوم التسيير

قسم العلوم الاقتصادية

مذكرة مقدمة لاستكمال متطلبات شهادة ماستر أكاديمي, الطور الثاني

في ميدان : العلوم الاقتصادية والتجارية وعلوم التسيير

فرع : العلوم الاقتصادية , التخصص: اقتصاد نقدي ومالي

بعنوان:

ادارة المخاطر السيبرانية في البنوك الجزائرية في ظل التحول الرقمي

دراسة حالة لفروع البنوك العمومية بورقلة (BEA – CPA – BNA)

من إعداد الطلبة :

أميرة منى الله قاضي

صفاء ريحانة زيتوني

نوقشت وأجيزت علنا بتاريخ: 2025/06/23

أمام اللجنة المكونة من السادة :

الأستاذ : د. هتهات السعيد	أستاذ محاضر (أ) – جامعة ورقلة – رئيسا
الأستاذ : د. نور الهدى حدادي	أستاذ محاضر (ب) – جامعة ورقلة – مشرفا و مقررا
الأستاذ : د. خالدي عصام	أستاذ محاضر (أ) – جامعة ورقلة – ممتحنا

السنة الجامعية: 2024-2025

جامعة قاصدي مرباح – ورقلة

كلية العلوم الاقتصادية والتجارية وعلوم التسيير

قسم العلوم الاقتصادية

مذكرة مقدمة لاستكمال متطلبات شهادة ماستر أكاديمي, الطور الثاني

في ميدان : العلوم الاقتصادية والتجارية وعلوم التسيير

فرع : العلوم الاقتصادية , التخصص: اقتصاد نقدي ومالي

بعنوان:

ادارة المخاطر السيبرانية في البنوك الجزائرية في ظل التحول الرقمي

دراسة حالة لفروع البنوك العمومية بورقلة (BEA – CPA – BNA)

من إعداد الطلبة :

أميرة منى الله قاضي

صفاء ريحانة زيتوني

نوقشت وأجيزت علنا بتاريخ: 2025/06/23

أمام اللجنة المكونة من السادة :

الأستاذ : د. هتهات السعيد	أستاذ محاضر (أ) – جامعة ورقلة – رئيسا
الأستاذ : د. نور الهدى حدادي	أستاذ محاضر (ب) – جامعة ورقلة – مشرفا و مقررا
الأستاذ : د. خالدي عصام	أستاذ محاضر (أ) – جامعة ورقلة – ممتحنا

السنة الجامعية: 2024I-2025

إهداء

إلى من غرَسوا في قلبي حب العلم، وسقوه بالصبر والدعاء والمساندة...

إلى من كانت سعادتي من سعادتهم، ونجاحي ثمرة تعبهم ورضاهم...

إلى أمي الحبيبة، نبض قلبي، وسرّ قوتي، التي كانت وما زالت الحضن الدافئ والدعاء الصادق، وسندي الأول في الحياة...

إلى أبي العزيز، نبع العطاء، وصاحب القلب الكبير، الذي علّمني أن الطموح لا سقف له، وأن الاجتهاد طريق الكرامة والنجاح...

إلى إخوتي وأخواتي، شركاء دربي وفرحتي، الداعمين بصمت، والمرابطين دومًا بجانبي رغم كل شيء...

إلى صديقتي الوحيدة، التي كانت النور في أوقات العتمة، والرفيقة التي لم تتخلّ، والكتف الذي استندت عليه في أصعب اللحظات...

وإلى صديقتي التي شاركتني هذا المشوار العلمي ورافقتني في إعداد هذه المذكرة، فكانت نعم المعينة، ونعم الرفيقة في التعب والنجاح... شكرًا لصدقك، لصبرك، ولكل لحظة دعم وتفاهم.

إلى أستاذتي المشرفة الفاضلة، التي لم تبخل عليّ بنصحها وتوجيهها، فكانت نِعم القدوة والعون...

وإلى كل أساتذتي الكرام، من مراحل دراستي الأولى وحتى هذا التتويج، الذين غرَسوا فيّ حب المعرفة، وغذّوا فيّ روح الباحث... كل التقدير والامتنان لكم جميعًا.

هذا التخرج هو ثمرة تعبنا جميعًا، فشكرًا من القلب... لكم جميعًا

صفاء ريحانة زيتوني

إهداء

بسم الله الرحمان الرحيم

يرفع الله الذين امنو منكم واللذين اوتو العلم درجات " المجادلة

نور دربي، سندي المتين في كل خطوة، أرفع هذا الإهداء بكل فخر و اعتزاز الى اعظم ام وأب فالكون ذرعي المتين نور عيني و نبض قلبي، ولكل أفراد عائلتي الأعزاء، من كانوا لي السند والأمان.

إلى العزيزة فاطمة واجمل اطفال ياسين وآدم وعبد رحيم، شكرًا لكم على حبكم ودعمكم الدائم. أدعو الله أن يحفظكم ويسعد أيامكم.

إلى عائلتي الثانية في ولاية ورقلة، إلى دار عمي محمد قاضي وكل أفراد أسرته، شكراً لكم على حبكم ودعمكم الدائم أنتم نعم الأهل والسند.

إلى صديقاتي العزيزات من الإقامة الجامعية: يمينة بالحبيب، شيماء زغيب ، فايزة هلالبة، جميلة بكوش ومنار بن صديق ، وكل من شاركني اجمل ايامي فالاقامة و كانو بهجة الروح.

ولا أنسى أبداً من رزقتوا بهن ,نعمة الله نورالهدى حليمي ، حفيظة دقيش، ورميسة.

قريشي و يعلمو انه لا كلمه تعبر عنهن او تصفن

كل الشكر والامتنان لرفيقتي في إعداد هذه المذكرة خفيفة الروح ريحانة زيتوني،

واجل بالشكر العظيم لأستاذتي المؤطرة نور الهدى حدادي، التي كانت لي النور والمرشدة في هذا الطريق.

وأخيراً، لكل من ساهم في مسيرتي التعليمية، شكراً من الأعماق.

أميرة من الله قاضي

شكر

إنه لمن تمام النُبل وصدق الوفاء أن نخصّ بالشكر والعرفان كل من كان لنا عونًا في إنجاز هذا العمل العلمي، وسندًا في بلوغ محطّة التخرّج.

نتوجه بجزيل الشكر والتقدير إلى رئيس قسم العلوم التجارية لما قدّمه من توجيه ودعم، وإلى كافة أساتذة التخصص على ما أتاحوه لنا من معارف قيّمة، وما بذلوه من جهود رصينة في مسارنا الجامعي، فقد كانوا لنا مشاعل علمٍ ونهجَ تميّز.

كما لا يفوتنا أن نثمّن كل لحظة تشاركنا فيها الجد والاجتهاد مع زملائنا وزميلاتنا في مقاعد الدراسة، سائلين الله تعالى أن يوفقهم جميعًا لما فيه خيرهم وسداد مسيرتهم.

وإن أسمى آيات التقدير نخصّ بها أستاذتنا الفاضلة نور الهدى حدادي، التي كانت لنا المؤطرة والداعمة، والقدوة في الجدية والتفاني، فلها منّا كل العرفان على صبرها، وإرشادها، وحسن عطائها.

نسأل الله أن يجزي الجميع عنا خير الجزاء، وأن يجعل هذا العمل خطوة مباركة في طريق العلم والعمل، ويكلل جهودنا جميعًا بالتوفيق والسداد.

الملخص

هدفت هذه الدراسة الى تحليل دور إدارة المخاطر السيبرانية في البنوك العمومية الجزائرية في ظل التحول الرقمي، وذلك من خلال تسليط الضوء على التحديات التي تواجهها هذه المؤسسات في تأمين بيئتها الرقمية المتنامية. وقد ركزت الدراسة على البنوك العمومية بولاية ورقلة كنموذج ميداني، بهدف تحليل مدى جاهزيتها في مواجهة التهديدات السيبرانية، وكذا رصد أوجه القصور في البنية التحتية، والتأطير البشري، والتنظيم الإداري.

اعتمدت الدراسة المنهج الوصفي التحليلي إلى جانب منهج دراسة الحالة، مستندة إلى مقابلات مع 8 موظفين من مختلف الإطارات مصرفية، حيث خلصت نتائجها الى وجود وعي أولي بالأمن السيبراني، يقابله غياب فعلي لأدوات الحماية المتكاملة، مما يعمّق من فجوة التحول الرقمي الآمن داخل هذه البنوك.

الكلمات المفتاحية:

أمن سيبراني، تحول رقمي، بنوك عمومية، مخاطر رقمية ، ورقلة .

Abstract

This study addresses the issue of cybersecurity risk management in Algerian public banks amid the ongoing digital transformation. It sheds light on the challenges these institutions face in securing their evolving digital environments. The research focuses on public banks in the Wilaya of Ouargla as a case study, aiming to assess their readiness to confront cyber threats and to identify gaps in infrastructure, human resources, and organizational frameworks.

The study adopts a descriptive-analytical approach, combined with the case study method. Based on interviews with banking executives, the findings reveal an initial awareness of cybersecurity issues, contrasted by the actual lack of integrated protection tools. This discrepancy exacerbates the vulnerability of digital transformation processes within these banks.

Keywords: Cybersecurity, Digital Transformation, Public Banks, Digital Risks, Ouargla.

قائمة المحتويات

قائمة المحتويات

قائمة المحتويات

قائمة الجداول:

قائمة الأشكال

المقدمة

01. توطئة

في ظل الثورة الرقمية التي تشهدها مختلف القطاعات الاقتصادية على مستوى العالم، برزت الحاجة الملحة إلى تطوير آليات متقدمة لحماية المؤسسات المالية من المخاطر الناجمة عن التهديدات السيبرانية. فمع تعاظم الاعتماد على التكنولوجيا الرقمية في تقديم الخدمات المصرفية، أصبح الأمن السيبراني ركيزة أساسية لضمان استمرارية الأعمال وحماية المعلومات الحساسة للعملاء، وهو ما دفع إلى ظهور إدارة المخاطر السيبرانية كعلم وفن يهدف إلى تقليل الخسائر المحتملة الناتجة عن الهجمات الإلكترونية التي تستهدف البنية التحتية الرقمية للمؤسسات المالية [1], وتُعد البنوك من أكثر المؤسسات عرضة لهذه المخاطر بسبب طبيعة عملها التي تتطلب تخزين ومعالجة كميات ضخمة من البيانات المالية الحساسة، مما يجعلها هدفًا رئيسيًا للهجمات السيبرانية. ويشير عبد القادر بن زيد إلى أن "إدارة المخاطر السيبرانية في البنوك هي عملية متكاملة تجمع بين السياسات التنظيمية والتقنيات التكنولوجية لتوفير بيئة مصرفية آمنة وقادرة على مواجهة التحديات الرقمية المتطورة".[2]

على الصعيد الوطني، شهد القطاع المصرفي الجزائري تحولات رقمية متسارعة أدت إلى تبني العديد من الخدمات الرقمية كأنظمة الدفع الإلكتروني والخدمات المصرفية عبر الإنترنت، الأمر الذي فتح المجال أمام فرص جديدة لتحسين جودة الخدمات المصرفية، لكنه في الوقت ذاته أفرز تحديات أمنية متزايدة تتطلب تعزيز إدارة المخاطر السيبرانية. إن الواقع الجزائري يعكس الحاجة الملحة إلى دراسة معمقة لهذا الجانب لضمان حماية النظام المالي من الأضرار التي قد تسببها الهجمات الإلكترونية , وقد تمّ اختيار فروع بعض البنوك العمومية الجزائرية في ولاية ورقلة كنموذج ميداني لتحليل واقع إدارة المخاطر السيبرانية، وذلك بالنظر إلى ما تشهده هذه الفروع من تحوّل رقمي متسارع في الخدمات البنكية، ولما تمثّله من امتداد فعلي للسياسات المركزية التي تنتهجها البنوك الأم. وتشمل هذه البنوك: البنك الوطني الجزائري (BNA)، بنك الفلاحة والتنمية الريفية (BADR)، القرض الشعبي الجزائري (CPA)، بنك التنمية المحلية (BDL)، والبنك الخارجي الجزائري (BEA). وقد مكّن هذا الاختيار من رصد مستوى التهديدات السيبرانية التي تواجهها هذه المؤسسات على المستوى المحلي، ومدى جاهزيتها لمواجهتها وفقًا لمتطلبات التحوّل الرقمي المعاصر.

---

[1] عبد القادر بن زيد، **إدارة المخاطر السيبرانية في المؤسسات المالية: دراسة تحليلية**، مجلة العلوم الاقتصادية، جامعة الجزائر، 2020، ص 45.

[2] عبد القادر بن زيد، المرجع السابق .

02. إشكالية الدراسة :

رغم الاهتمام المتزايد بالأمن السيبراني على المستوى العالمي، يظل التحدي الأكبر هو كيفية تكيف المؤسسات المالية، وبشكل خاص البنوك الجزائرية، مع التغيرات الرقمية المتسارعة التي تفرضها الثورة التكنولوجية. فإلى جانب الفرص الهائلة التي تتيحها هذه التحولات في تحسين الخدمات المصرفية، تواجه البنوك تحديات متزايدة في حماية بنيتها التحتية الرقمية من التهديدات السيبرانية المتطورة باستمرار. لذا، تبرز إشكالية محورية تتلخص في التساؤل التالي:

كيف تتعامل البنوك الجزائرية مع المخاطر السيبرانية في ظل التحول الرقمي؟

03. التساؤلات الفرعية

بناءً على التساؤل العام، تبرز مجموعة من التساؤلات الفرعية التي تسعى هذه الدراسة إلى الإجابة عنها، وهي:

- ما هي طبيعة المخاطر السيبرانية التي تواجه البنوك الجزائرية؟
- ما مدى جاهزية البنوك الجزائرية لمواجهة هذه التهديدات في ظل التحول الرقمي؟
- ما هي الإستراتيجيات والآليات المعتمدة من قبل البنوك الجزائرية لإدارة المخاطر السيبرانية؟
- ما هي أبرز التحديات التي تعيق التطبيق الفعّال لإدارة المخاطر السيبرانية في القطاع المصرفي الجزائري؟

04. الفرضيات

بناءً على الإشكالية المطروحة والتساؤلات الفرعية المتفرعة عنها، ومن خلال القراءة التحليلية الأولية للواقع السيبراني في القطاع المصرفي الجزائري، فإن هذه الدراسة تنطلق من مجموعة من الفرضيات على النحو التالي:

- تواجه البنوك الجزائرية مخاطر سيبرانية متزايدة نتيجة التوسع المستمر في استخدام التكنولوجيات الرقمية والخدمات المصرفية الإلكترونية، مما يزيد من مستوى التهديدات الموجهة إلى نظمها المعلوماتية.
- تعتمد البنوك الجزائرية على مجموعة من الوسائل والآليات لإدارة المخاطر السيبرانية، غير أنها لا تزال تعاني من عدة نقائص على مستوى الكفاءات البشرية، والجاهزية التقنية، وكفاءة أنظمة الحماية.
- يشكّل غياب إطار تنظيمي موحد ونقص التكوين المتخصص في الأمن السيبراني أحد أبرز العوائق التي تحدّ من فعالية تطبيق سياسات إدارة المخاطر السيبرانية في البنوك الجزائرية.
- يُعتبر التكامل بين التحول الرقمي واستراتيجية الأمن السيبراني عنصرًا حاسمًا في تعزيز قدرة البنوك الجزائرية على مواجهة المخاطر السيبرانية، وذلك انطلاقًا مما تكشف عنه المعطيات الميدانية وآراء الفاعلين في القطاع البنكي.

05. أسباب اختيار موضوع الدراسة

أولا الأسباب الذاتية

- رغبة الباحثتين في التعمق في موضوع حديث وذو أهمية متزايدة في مجال الأمن السيبراني.
- اهتمام الطالبات بالتكنولوجيا وتأثيرها على القطاع المالي.
- الرغبة في المساهمة في تطوير القطاع المصرفي الجزائري من خلال البحث العلمي.
- رغبة في تطوير المهارات البحثية العملية من خلال الدراسة الميدانية والمقابلات.

ثانيا: الأسباب الموضوعية

- تزايد الاعتماد على الخدمات الرقمية في البنوك الجزائرية مما يرفع من أهمية إدارة المخاطر السيبرانية.
- الحاجة الملحة لتقييم واقع السياسات والإجراءات المعتمدة في البنوك الجزائرية، خاصة بفروع ولاية ورقلة.
- نقص الدراسات الميدانية التي تعالج موضوع الأمن السيبراني في البنوك المحلية.
- الأهمية الاقتصادية والاجتماعية لولاية ورقلة كمركز مصرفي يستوجب دراسة خصوصياتها.
- التحديات التي تواجه البنوك الجزائرية في مجال الأمن السيبراني، من حيث نقص الإطار التنظيمي والكفاءات.
- إمكانية تقديم توصيات عملية تساعد في تعزيز آليات حماية المعلومات والأنظمة المصرفية.

06. أهمية الدراسة

أولًا: الأهمية العلمية

تنبع الأهمية العلمية لهذه الدراسة من الاعتبارات الآتية:

- الإسهام في إثراء الأدبيات النظرية المتعلقة بإدارة المخاطر السيبرانية في السياق البنكي، من خلال تسليط الضوء على مفاهيم جديدة ترتبط بالأمن السيبراني في ظل التحول الرقمي، وهو مجال لا يزال قيد التبلور في البيئة الأكاديمية العربية عامة والجزائرية خاصة.
- محاولة الربط بين متغيرين مركزيين هما التحول الرقمي وإدارة المخاطر السيبرانية، مما يمنح للدراسة طابعًا تفسيريًا وتحليليًا متقدمًا يُسهم في تطوير فهم علمي معمّق للعلاقة بين التقدم التكنولوجي البنكي من جهة، ومستوى الجاهزية السيبرانية من جهة أخرى.
- سدّ فجوة بحثية قائمة في ميدان الدراسات السيبرانية البنكية، من خلال تقديم دراسة ميدانية نوعية تعتمد على مقابلات مباشرة مع الفاعلين في القطاع البنكي، وهو أسلوب قلّما تم اعتماده في الدراسات السابقة التي غلبت عليها المقاربات الكمية أو التحليل الثانوي للبيانات.

ثانيًا: الأهمية العملية

أما من حيث الأهمية العملية، فتتمثل في:

- إبراز التحديات الواقعية التي تواجهها البنوك الجزائرية في سبيل تأمين بنيتها التحتية الرقمية وحماية بياناتها ومصالح زبائنها، مما يساعد في صياغة ملاحظات ميدانية ذات طابع توجيهي لصنّاع القرار.
- تقديم مجموعة من التوصيات القابلة للتنفيذ لفائدة مسؤولي البنوك ومخططي السياسات المالية الرقمية، تساعد على تحسين جاهزية النظام البنكي الجزائري لمواجهة التهديدات السيبرانية.
- دعم جهود التحول الرقمي الآمن في القطاع المصرفي، من خلال المساهمة في بلورة تصور شامل لإدارة المخاطر في بيئة تعتمد بشكل متزايد على النظم التكنولوجية، وهو ما يتماشى مع التوجهات الوطنية نحو الرقمنة.

07. أهداف الدراسة :

- تحليل واقع المخاطر السيبرانية في الفروع البنكية بولاية ورقلة: التعرف على طبيعة التهديدات السيبرانية التي تواجه فروع البنوك الكبرى في الولاية مثل بنك الجزائر الخارجي(BEA) ، وبنك القرض الشعبي الجزائري (CPA)، والبنك الوطني الجزائري.(BNA)
- تقييم مدى جاهزية الفروع: دراسة مدى استعداد الفروع المحلية في ورقلة من حيث البنية التحتية التقنية والإجراءات الأمنية لمواجهة المخاطر السيبرانية.
- استقصاء استراتيجيات إدارة المخاطر لدى الفروع: تحليل السياسات والتدابير الأمنية المطبقة في فروع البنوك المختارة، ومدى فعاليتها في التعامل مع التهديدات الرقمية.
- تحديد التحديات الخاصة بالفروع المحلية: الكشف عن المعوقات التنظيمية، الفنية، والبشرية التي تعيق تطبيق إدارة مخاطر سيبرانية فعالة في فروع ولاية ورقلة.
- اقتراح توصيات عملية لتطوير أمن المعلومات في الفروع: تقديم حلول وإجراءات ملموسة لتعزيز الحماية السيبرانية وتحسين آليات إدارة المخاطر في فروع البنوك بولاية ورقلة، بما يتناسب مع واقع التحول الرقمي

08. هيكل الدراسة

يتضمن هذا البحث فصلين رئيسيين يُعالج كل منهما جانبًا محوريًا من موضوع الدراسة. تناول الفصل الأول الجانب النظري، حيث خُصص المبحث الأول لتأصيل الإطار المفاهيمي لمتغيرات الدراسة، من خلال تعريف وتحليل مفاهيم الأمن السيبراني، التحول الرقمي، وإدارة المخاطر السيبرانية، مع توضيح طبيعة العلاقة بينها في السياق المصرفي الجزائري. أما المبحث الثاني فقد تضمن استعراضًا منهجيًا للدراسات السابقة، سواء العربية أو الأجنبية، ذات الصلة بالموضوع، بغرض استخلاص أهم النتائج التي توصلت إليها، وتحديد الفجوات البحثية التي تسعى هذه الدراسة إلى سدها. أما الفصل الثاني فقد تناول الجانب التطبيقي للدراسة، حيث خُصص المبحث الأول لوصف خصائص العينة، وتوضيح منهجية وأدوات الدراسة المعتمدة، في حين ركز المبحث الثاني على عرض وتحليل ومناقشة نتائج المقابلات الميدانية التي أُجريت مع إطارات البنوك العمومية بورقلة، وذلك في ضوء فرضيات الدراسة ومحاورها الأساسية، مع الاستناد إلى ما تم رصده من معطيات واقعية ومؤشرات نوعية تعبّر عن واقع إدارة المخاطر السيبرانية في ظل التحول الرقمي داخل هذه المؤسسات.

الفصل الأول :

الإطار النظري لإدارة المخاطر السيبرانية في البنوك الجزائرية

تمهيد :

تُعد إدارة المخاطر السيبرانية من المحاور الحيوية التي تكتسب أهمية متزايدة في القطاع المصرفي، لا سيما في ظل التوسع المتسارع للتحول الرقمي واعتماد الخدمات الإلكترونية. فالبنوك، باعتبارها مؤسسات مالية تحتفظ بمعطيات حساسة وتدير عمليات مالية معقدة، تواجه تهديدات متطورة تتطلب آليات فعالة للتصدي لها وضمان استمرارية العمل. لذا، يتطلب الأمر توضيح المفاهيم الأساسية المتعلقة بالأمن السيبراني وأنواع المخاطر المرتبطة به، بالإضافة إلى فهم العلاقة التفاعلية بين التحول الرقمي وإدارة هذه المخاطر. كما يشمل هذا الفصل مراجعة الدراسات السابقة التي تناولت هذا المجال، بهدف الاستفادة من الخبرات البحثية السابقة وتحديد الفجوات التي تفتح آفاقاً للدراسة الحالية. من خلال ذلك، يتضح السياق العلمي الذي تستند إليه الدراسة، ويوفر إطاراً منظماً لتحليل الواقع التطبيقي في الفصول التالية.

المبحث الأول: الإطار المفاهيمي لمتغيرات الدراسة

تتطلب دراسة إدارة المخاطر السيبرانية في البنوك الجزائرية فهماً دقيقاً للمفاهيم الأساسية المرتبطة بهذه الظاهرة، والتي تشكل الأساس النظري والتحليلي لفهم واقع التحديات الأمنية التي تواجه البنوك في ظل التحول الرقمي المتسارع. لذلك، يشتمل هذا المبحث على تعريف شامل لمفهوم إدارة المخاطر السيبرانية، مع التعمق في خصائص هذا المفهوم في السياق البنكي، ثم عرض مفصل لمفهوم التحول الرقمي في البنوك الجزائرية، وأخيراً تناول العلاقة التفاعلية بين المتغيرين.

المطلب الأول: المفاهيم العامة لإدارة المخاطر السيبرانية في البنوك

لفهم طبيعة إدارة المخاطر السيبرانية في البنوك، يشتمل علنا توضيح الجوانب المفاهيمية المتعددة لهذا المجال المعقد و اللذي يعد نقطة انطلاق أساسية ، بحيث التطرق لمفهوم المخاطر السيبرانية، مكونات إدارة هذه المخاطر، وأهميتها الاستراتيجية في المؤسسات المصرفية.

الفرع الأول: مفهوم المخاطر السيبرانية وأنواعها

في ظل التحول الرقمي المتسارع الذي تشهده المؤسسات المعاصرة، أصبحت الأنظمة الرقمية عصبًا أساسيًا في أداء المهام التشغيلية والإدارية، وهو ما جعلها عرضة دائمة لمخاطر من نوع جديد تُعرف بـ"المخاطر السيبرانية". ويُفهم من المصطلح لغويًا أنه يشير إلى كل ما يهدد الفضاء الإلكتروني ويُعرّض سلامته ووظيفته للخطر. أما من الناحية الاصطلاحية، فقد عرّف Gordon & Loeb المخاطر السيبرانية بأنها:

"الاحتمالات التي تؤدي إلى فقدان البيانات أو تعطيل العمليات أو انتهاك الخصوصية أو تلف السمعة نتيجة ثغرات أو هجمات على البنية التحتية الرقمية".[1]

وفي هذا السياق، تتجلى إدارة المخاطر السيبرانية كنهج استراتيجي شامل يهدف إلى التعرف على تلك التهديدات وتقييم آثارها المحتملة ووضع آليات للوقاية منها أو التخفيف من أضرارها. وقد أوضح Pfleeger & Pfleeger أن إدارة هذه المخاطر تتطلب" :تبني مزيج من السياسات التقنية والإدارية التي تؤسس لبيئة رقمية آمنة، قائمة على التنبّه المستمر وتحديث أدوات الحماية، ضمن منظور ديناميكي يتكيف مع طبيعة التهديدات المتغيرة".[2] وتكتسي هذه الإدارة أهمية خاصة في المؤسسات المصرفية، التي تُعد من أكثر القطاعات استهدافًا

[1] Gordon, L. A., & Loeb, M. P. (2002). **The Economics of Information Security Investment**. ACM Transactions on Information and System Security, 5(4), p. 443.
[2] Pfleeger, C. P., & Pfleeger, S. L. (2012**). Security in Computing.** 5th ed. Pearson Education, p. 189.

بالهجمات الإلكترونية، نظرًا لحساسية البيانات التي تتعامل معها والطبيعة الحرجة للخدمات التي تقدمها. فقد أكدتChristine Lagarde ، الرئيسة السابقة لصندوق النقد الدولي، أن:

"التهديدات السيبرانية تُعد الخطر النظامي الأبرز الذي يهدد الاستقرار المالي العالمي، لا سيما في القطاع المصرفي"[1] ,وفي ذات السياق، شددت منظمة التعاون الاقتصادي والتنمية (OECD) على أن الاستجابة الفعالة لتلك التهديدات تتطلب من البنوك اعتماد أطر مؤسسية واضحة لإدارة المخاطر، تتضمن تقييمًا دوريًا للثغرات، تدريبًا مستمرًا للموظفين، وتطويرًا متواصلًا للبنية التحتية الأمنية.[2] وتتنوع أشكال المخاطر السيبرانية التي تواجهها المؤسسات المصرفية، ويأتي على رأسها البرمجيات الخبيثة(Malware) ، ومحاولات التصيد الاحتيالي (Phishing)، وهجمات حجب الخدمة(DDoS) ، فضلًا عن التهديدات الداخلية التي قد تصدر عن موظفين أو متعاونين لديهم صلاحيات وصول للأنظمة الرقمية. وقد أشارBruce Schneier ، أحد أبرز خبراء أمن المعلومات، إلى أن:

"أخطر أنواع الهجمات السيبرانية ليست تلك التي تأتي من الخارج فقط، بل تلك التي تُنفذ من داخل المؤسسة باستخدام صلاحيات نظامية وبأساليب يصعب تتبعها".[3] كل التهديدات الرقمية المحتملة التي يمكن أن تستهدف البنية التحتية للمصارف الجزائرية، قد تُفضي إلى خسائر مالية مباشرة، أو تسريب بيانات سرية، أو إعاقة تقديم الخدمات البنكية، سواء صدرت هذه التهديدات من جهات خارجية أو داخلية، وسواء كانت متعمدة أو ناتجة عن ثغرات أمنية غير مقصودة. وتُقاس هذه المخاطر من خلال عدة مؤشرات أهمها: توفر السياسات الأمنية داخل المؤسسة، كفاءة فرق الأمن السيبراني، جهوزية البنية الرقمية، ومستوى التكوين والتحسيس لدى المستخدمين. وقد أظهرت دراسات ميدانية جزائرية متخصصة أن أبرز العوائق أمام تحقيق إدارة فعالة للمخاطر السيبرانية في البنوك الوطنية تكمن في محدودية الكفاءات التقنية، وغياب إطار تنظيمي موحد، بالإضافة إلى ضعف التنسيق بين الجهات المعنية بالحماية الرقمية.[4]

إذ نستخلص مما سبق أن إدارة المخاطر السيبرانية لم تعد خيارًا مؤسساتيًا بل ضرورة إستراتيجية لحماية البنوك من التهديدات المتزايدة والمعقدة في البيئة الرقمية، وأن نجاحها رهين بقدرة المؤسسة على التكيف السريع، وتبني نظم حماية متعددة المستويات، وتفعيل آليات التقييم المستمر للمخاطر.

[1] Lagarde, C. (2017). **"The Financial Sector Must Take Cyber Risk More Seriously"**. World Economic Forum.

[2] OECD (2021**). Cybersecurity Risk Management for Financial Stability**, p. 5.

[3] Schneier, B. (2015). Data and Goliath: **The Hidden Battles to Collect Your Data and Control Your World. Norton & Company**, p. 114.

[4] المديرية العامة لأمن نظم المعلومات، **تقرير داخلي غير منشور** ، وزارة الرقمنة والإحصائيات، الجزائر، 2023، ص 32.

الفرع الثاني: مكونات إدارة المخاطر السيبرانية في البنوك

تُبنى إدارة المخاطر السيبرانية على مجموعة من المكونات الأساسية التي تُمثّل الإطار العملي والتنظيمي لمجابهة التهديدات الرقمية، خاصة في المؤسسات البنكية التي تعتمد بشكل شبه كامل على أنظمة رقمية متداخلة ومعقدة. هذه المكونات لا تُعتبر فقط أدوات تقنية، بل هي سياسة مؤسساتية تُترجم في الواقع إلى هياكل إدارية وإجراءات تشغيلية تنسجم مع طبيعة المخاطر وتطورها."فعالية إدارة المخاطر السيبرانية في البنوك الجزائرية لا تُقاس فقط بامتلاك تكنولوجيا حديثة، بل تتوقف أساسًا على مدى تكامل مكونات هذه الإدارة داخل الهيكل العام للمؤسسة البنكية".[1]

وعليه، يمكن تحديد أبرز مكونات إدارة المخاطر السيبرانية في البنوك على النحو التالي:

– سياسة أمن المعلومات(Information Security Policy) : تمثل هذه السياسة القاعدة التنظيمية لإدارة كل ما يتعلق بأمن البيانات داخل البنك، حيث تُعرّف الصلاحيات، وتُحدّد مستويات الوصول، وتُنظّم سلوكيات العاملين في التعامل مع الأنظمة الرقمية. وتُعدّ هذه السياسة من المكونات الحاسمة في الوقاية من الهجمات الإلكترونية الداخلية والخارجية.

ويُشير الدكتور عبد المجيد بوقرة في كتابه "الأمن السيبراني في المؤسسات المالية العربية" إلى أن "غياب سياسة واضحة ومحدثة لأمن المعلومات يفتح المجال أمام العديد من الثغرات التنظيمية والتقنية، خصوصًا في ظل بيئة مصرفية تتطور رقميًا بسرعة أكبر من قدرتها على المواكبة المؤسسية".[2]

– تحليل وتقييم المخاطر(Risk Assessment and Analysis) : وهو الجانب التشخيصي الذي يسمح للمؤسسة البنكية بالتعرف على نقاط الضعف في بنيتها الرقمية وتحديد مصادر التهديد. ويتم هذا من خلال تحليل سيناريوهات محتملة للهجوم، وتقدير أثرها، وتقييم احتمال حدوثها. هذه العملية تُعدّ الخطوة المنهجية التي تسبق اتخاذ أي إجراء وقائي أو علاجي.

في هذا الإطار، توصي اللجنة الجزائرية للرقابة المصرفية (COSOB) في أحد منشوراتها الفنية بأن "تحليل المخاطر يجب أن يُبنى على معايير كمية ونوعية ويشمل جميع أصول البنك الرقمية دون استثناء، مع مراجعة دورية لنتائجه".[1]

---

[1] بركات سارة، ودبلة فاتح (2015)، **دور تطبيق الإجراءات الاحترازية لإدارة المخاطر البنكية في تحسين الحوكمة المصرفية**: دراسة حالة بنك سوسيتي جنرال الجزائر، رسالة دكتوراه، جامعة خيضر –بسكرة، ص. 417.

[2] عبد المجيد بوقرة، **الأمن السيبراني في المؤسسات المالية العربية**، دار الخلدونية، الجزائر، 2020، ص. 57.

– **الاستجابة للحوادث السيبرانية(Incident Response)** : وهي الإجراءات التي تُتّخذ بمجرد حدوث تهديد أو اختراق إلكتروني، وتشمل آليات الاكتشاف المبكر، التبليغ، التحقيق، والتعافي. وتُعد هذه الاستجابة عنصرًا محوريًا في تقليص الأضرار المباشرة وغير المباشرة التي قد تنجم عن الاختراقات.

وتؤكد دراسة محمد بن صالح أن "ضعف فرق الاستجابة السيبرانية في البنوك الجزائرية ناتج عن غياب التدريب المستمر وضعف التعاون بين الإدارة العامة ووحدة أمن المعلومات".[2]

– **التوعية والتكوين المستمر** : يُعتبر العامل البشري من أبرز نقاط الضعف في البنية السيبرانية للمؤسسات، ولذلك فإن توعية الموظفين وتدريبهم على التعامل السليم مع البيانات والأنظمة يُعد من أهم مكونات الإدارة الناجعة للمخاطر. وغالبًا ما تكون الهجمات السيبرانية ناجحة بسبب ثغرات سلوكية، لا تقنية.

وقد شدد الباحث الجزائري محمد بلقاسم في ورقته البحثية حول المخاطر السيبرانية في البنوك المغاربية على أن "الثقافة الأمنية المعلوماتية غائبة عن معظم موظفي القطاع المصرفي، مما يجعلهم الحلقة الأضعف في منظومة الدفاع الرقمي"[3].

الفرع الثالث: مراحل إدارة المخاطر السيبرانية في البنوك الجزائرية

تمر إدارة المخاطر السيبرانية في البنوك الجزائرية بعدة مراحل متكاملة تسهم في الحد من التهديدات الإلكترونية وحماية الأصول الرقمية، وهي مراحل تم تحديدها بناءً على مراجعة الأدبيات والدراسات المحلية والعربية المختصة في مجال الأمن السيبراني البنكي.

– **المرحلة الأولى التعرف على المخاطر(Risk Identification)** : في هذه المرحلة، يتم جمع المعلومات حول جميع التهديدات المحتملة التي قد تؤثر على أنظمة المعلومات الرقمية للبنك. تشمل المخاطر تقنيات الاختراق، البرمجيات الخبيثة، سرقة البيانات، والهجمات التي تستهدف البنية التحتية التقنية. وفقًا لمذكرة ماجستير

---

[1] اللجنة الجزائرية للرقابة المصرفية (COSOB)، **نشرة تنظيمية حول التحديات الرقمية للبنوك**، العدد03، الجزائر،2022،ص19.

[2] محمد بن صالح , مذكرة ماجستير: تحليل واقع المخاطر السيبرانية في البنوك العمومية الجزائرية، كلية الاقتصاد، جامعة ورقلة، 2021، ص. 34.

[3] محمد بلقاسم، "**المخاطر السيبرانية في النظام البنكي المغاربي: التحديات والحلول**"، مجلة الاقتصاد الرقمي المغاربي، العدد 5، جامعة سوق أهراس، 2022، ص. 48.

بعنوان "تحليل واقع المخاطر السيبرانية في البنوك العمومية الجزائرية"، فإن التعرف الدقيق على هذه المخاطر يشكل حجر الأساس لأي نظام فعال لإدارة المخاطر.[1]

– المرحلة الثانية تقييم وتحليل المخاطر(Risk Assessment and Analysis) : بعد تحديد المخاطر، تأتي مرحلة تقييم حجم وتأثير كل منها. يتضمن ذلك دراسة احتمالية حدوث الهجوم وتأثيره المالي والتشغيلي على البنك. وتساعد هذه المرحلة على ترتيب الأولويات وتحديد الموارد المناسبة للتعامل مع كل خطر. وتؤكد دراسة "فاعلية استراتيجيات الأمن السيبراني في البنوك الجزائرية" على أهمية استخدام معايير تقييم موحدة لضمان دقة التقدير[2].

– المرحلة الثالثة تطوير استراتيجيات التحكم في المخاطر(Risk Control Strategies) : تتضمن هذه المرحلة وضع الخطط والسياسات والتدابير التقنية اللازمة لتقليل المخاطر المكتشفة إلى مستوى مقبول. وتتنوع هذه الاستراتيجيات بين تطبيق أنظمة جدران الحماية، تحديث البرمجيات، توعية الموظفين، واعتماد بروتوكولات الأمان المتقدمة. كما أشارت مذكرة جامعة ورقلة إلى أن البنوك الجزائرية ما تزال في طور تطوير هذه الاستراتيجيات بشكل متكامل وموحد.[3]

المرحلة الرابعة: التنفيذ والمتابعة(Implementation and Monitoring) : تشمل تطبيق استراتيجيات التحكم ومراقبة فعاليتها بشكل مستمر من خلال أنظمة مراقبة واختبار اختراق دوري، والتأكد من التزام جميع العاملين بسياسات الأمن. ويرى الباحث حمدي بن عاشور أن المتابعة المستمرة تُعد من أهم عوامل نجاح إدارة المخاطر السيبرانية، حيث تكشف عن نقاط الضعف المستجدة وتسمح بالتحديث المستمر للخطط.[4]

المرحلة الخامسة: الاستجابة والتعافي(Response and Recovery) : تتعامل هذه المرحلة مع كيفية الاستجابة الفورية للهجمات السيبرانية وتقليل أضرارها، بالإضافة إلى خطط التعافي لاستعادة العمليات الطبيعية للبنك بأسرع وقت ممكن. ويبرز في هذا الصدد أهمية وجود فريق متخصص للطوارئ السيبرانية، كما هو متبع في البنوك الكبرى حول العالم، مع ضرورة تدريب فرق الأمن على سيناريوهات متنوعة.[5]

---

[1] محمد بلقاسم , المرجع السابق , ص34.

[2] جمال بوازدية , مذكرة ماستر بعنوان : "**فاعلية استراتيجيات الأمن السيبراني في البنوك الجزائرية**"، كلية العلوم الاقتصادية، جامعة الجزائر 3، 2021، ص. 12.

[3] حمدي بن عاشور، **الأمن السيبراني في المؤسسات المالية**، 2020، ص. 45.

[4] نفس المرجع السابق، حمدي بن عاشور، 2020، ص. 57.

[5] منظمة التعاون الاقتصادي والتنمية (OECD)، **تقرير الأمن السيبراني للنظام المالي**، 2019، ص. 21.

المطلب الثاني: التحول الرقمي في البنوك الجزائرية

يشكّل التحول الرقمي أحد أبرز التحولات الاستراتيجية التي تشهدها البنوك في العالم، إذ أضحى ضرورة ملحّة لمواكبة التطورات التكنولوجية المتسارعة وتلبية توقعات العملاء المتزايدة بشأن الخدمات البنكية الذكية. وفي السياق الجزائري، بدأت المؤسسات المصرفية تخطو نحو رقمنة خدماتها، رغم وجود تحديات تنظيمية وتقنية وبشرية تعيق المسار أحيانًا. وعليه، سنتناول في هذا المطلب طبيعة هذا التحول ومؤشراته، ونتوقف عند العوامل المؤثرة فيه، لننتقل إلى دراسة معيقاته في البيئة الجزائرية.

الفرع الأول: مفهوم التحول الرقمي في البنوك وأبعاده

– أولاً : مفهوم التحول الرقمي في البنوك : يُعد التحول الرقمي في البنوك من أبرز مظاهر التغيير المؤسسي في ظل الاقتصاد الرقمي. ويُقصد به ذلك الانتقال الاستراتيجي الذي تتبناه المؤسسات المالية من خلال دمج التقنيات الرقمية في مختلف أنشطتها التشغيلية والخدماتية، بهدف تحسين الكفاءة التشغيلية، وتعزيز تجربة العميل، وضمان الاستمرارية في بيئة تتسم بالتطور السريع للتكنولوجيا.

يُشتق مصطلح "التحول" من الجذر "حوّل"، أي غيّر، ومنه يُفهم أن التحول الرقمي هو عملية تغيير جذرية باستخدام الوسائل الرقمية.

التعريف الاول عرفته منظمة الإنتربنك (**Interbank**) : **"تبنّي البنوك لتقنيات رقمية متقدمة في نظمها الداخلية والخارجية، تشمل البنية التحتية، وواجهات التفاعل مع العملاء، ونماذج الأعمال، بهدف تقديم خدمات مالية مبتكرة بشكل أسرع وأكثر أمانًا"**.[1] و يرى الدكتور عبد الحكيم العمري أن التحول الرقمي في البنوك هو **"عملية متكاملة تشمل إعادة تصميم الإجراءات البنكية التقليدية عبر استخدام تكنولوجيا المعلومات والاتصال، بهدف تحسين فعالية الأنشطة البنكية، وتسهيل المعاملات المالية من خلال قنوات إلكترونية مؤمنة"**.[2]

[1] منظمة Interbank الدولية، **تقرير "Digital Transformation in Financial Sector"**، ص. 6.

[2] عبد الحكيم العمري، **الرقمنة والتحول في المؤسسات المصرفية العربية**، دار صفاء للنشر، عمان، 2020، ص. 41.

التعريف الثاني "**مسار تدريجي يهدف إلى رقمنة العمليات البنكية، اعتمادًا على منصات إلكترونية وقنوات رقمية مثل التطبيقات البنكية، والخدمات المصرفية عبر الإنترنت، وأجهزة الصراف الآلي الذكية**".[1]

التعريف الثالث **;** "**التحول الرقمي في البنوك الجزائرية لا يقتصر على الأتمتة فقط، بل يشمل التغيير في الثقافة التنظيمية، وتطوير المهارات البشرية، وتبني نماذج أعمال رقمية أكثر تفاعلية**".[2]

ومن خلال ما سبق، يمكننا تعريف التحول الرقمي بأنه :

"**العملية التي تعتمد من خلالها البنوك الجزائرية على التكنولوجيا الرقمية لتطوير بنيتها التحتية، وتحسين جودة الخدمات البنكية، وتعزيز القدرة التنافسية، مع مراعاة التغيرات التشريعية والتقنية والبشرية التي تواكب هذا التحول**".

– ثانياً ; أبعاد التحول الرقمي في البنوك : يشمل التحول الرقمي في البنوك جملة من الأبعاد المتكاملة، التي توضح مدى شمولية وتأثير هذا المسار في الواقع المصرفي. ويمكن تلخيصها في الأبعاد الآتية:

- **البعد التكنولوجي**: يُعد العمود الفقري للتحول الرقمي، حيث يشمل تطوير البنية التحتية التكنولوجية، مثل أنظمة الحوسبة السحابية، الذكاء الاصطناعي، تقنيات البلوك تشين، وتطبيقات الهواتف الذكية.[3]
- **البعد التنظيمي**: يتمثل في إعادة هندسة العمليات الداخلية وإعادة هيكلة النظام الإداري والوظيفي ليتوافق مع التحول الرقمي، من حيث الحوكمة والرقابة الإلكترونية.[4]
- **البعد البشري**: يشير إلى ضرورة تدريب وتأهيل الكفاءات البشرية للتفاعل بكفاءة مع الأنظمة الرقمية، كما يتضمن التحول في الثقافة التنظيمية نحو بيئة رقمية مرنة.[5]
- **البعد القانوني**: يقتضي وجود إطار تشريعي منظم يضمن أمان المعاملات الرقمية، ويحفظ حقوق العملاء، وينظم العلاقة بين البنك والمستخدم الرقمي.[6]

---

[1] سارة بن قادة، سهام بوجلال، **فاعلية استراتيجيات الأمن السيبراني في البنوك الجزائرية**، مذكرة ماجستير، جامعة الجزائر 3، كلية العلوم الاقتصادية، 2021، ص. 12.

[2] عبد القادر شريف، التحول الرقمي كأداة للابتكار في البنوك الجزائرية، مجلة الدراسات المالية والمصرفية، جامعة باتنة، العدد 6، 2022، ص. 19.

[3] نفس المرجع السابق، ص. 21.

[4] عبد الحكيم العمري، نفس المرجع السابق، ص. 45.

[5] بن قادة، بوجلال، نفس المرجع السابق، ص. 15.

[6] نفس المرجع السابق، ص. 16.

- **البعد الأمني**: يرتبط بالحماية السيبرانية لأنظمة البنوك، وضمان سرية المعلومات، وحماية البيانات من القرصنة والاختراقات.[1]

وقد اكدت عدة دراسات أن التحول الرقمي في البنوك الجزائرية ما يزال يواجه صعوبات تتعلق بالأبعاد البشرية والتنظيمية، رغم التقدم الملموس في البنية التحتية الرقمية.[2]

الفرع الثاني: دوافع وأهداف التحول الرقمي في البنوك الجزائرية

أصبح التحول الرقمي في القطاع البنكي من أبرز القضايا الاستراتيجية التي تفرض نفسها في ظل التحولات العالمية المتسارعة، والتطور المستمر لتكنولوجيا المعلومات والاتصال. وتزايدت أهمية هذا التحول في البيئة الجزائرية بالنظر إلى ما يشهده العالم من انتقال إلى اقتصاد رقمي يرتكز على الابتكار، وسرعة المعاملات، وأمن المعلومات.

– أولاً : دوافع التحول الرقمي في البنوك الجزائرية : إن الدوافع التي تقف خلف سعي البنوك الجزائرية إلى اعتماد استراتيجيات التحول الرقمي متعددة، ويمكن تلخيص أبرزها فيما يلي:

- **مواكبة التطورات التكنولوجية العالمية:** حيث تسعى البنوك الجزائرية إلى تقليص الفجوة الرقمية التي تفصلها عن المؤسسات المالية العالمية، وخاصة في ظل الثورة الصناعية الرابعة التي أعادت تشكيل نموذج العمل المصرفي بشكل جذري.[3]
- **تحقيق الكفاءة التشغيلية:** تُمكّن الأنظمة الرقمية البنوك من أتمتة العمليات وتقليل الاعتماد على المعاملات الورقية، مما يساهم في تقليص التكاليف وزيادة الإنتاجية.[4]
- **تحسين تجربة العملاء:** يشكل التحول الرقمي أداة فعالة لتقديم خدمات مصرفية آنية وسلسة للعملاء، مع إتاحة منصات إلكترونية تتيح إجراء مختلف المعاملات دون الحاجة للتنقل إلى الفروع التقليدية.[5]
- **الاستجابة للمنافسة المحلية والإقليمية:** إذ لم يعد بإمكان البنوك الجزائرية الصمود في وجه المؤسسات المالية الأجنبية التي دخلت السوق الوطنية، دون أن تطور نماذج رقمية متقدمة.[6]

---

[1] شريف، نفس المرجع السابق، ص. 22

[2] طويري، صباح ومداني، سماح سعدية،**تحليل واقع التحول الرقمي في البنوك العمومية الجزائرية**، مذكرة ماجستير، جامعة ورقلة، كلية الاقتصاد، 2021، ص. 34.

[3] بوزادية جمال، "**فاعلية استراتيجيات الأمن السيبراني في البنوك الجزائرية**"، كلية العلوم الاقتصادية، جامعة الجزائر 3، 2021، ص. 13.

[4] نفس المرجع السابق، ص. 14.

[5] بن عيسى سميرة، "**التحول الرقمي في البنوك الجزائرية كآلية لتحسين جودة الخدمة المصرفية**"، مذكرة ماجستير، جامعة البليدة 2، كلية العلوم الاقتصادية، 2020، ص. 42.

[6] نفس المرجع السابق، ص. 44.

- **تعزيز الأمن السيبراني:** فالتقنيات الرقمية الحديثة تتيح للبنوك أدوات متطورة لرصد التهديدات وحماية البيانات، مما يجعل التحول الرقمي أيضًا جزءًا من استراتيجية الأمن.[1]

– ثانياً ; أهداف التحول الرقمي في البنوك الجزائرية: يهدف التحول الرقمي في البنوك الجزائرية إلى تحقيق مجموعة من النتائج الجوهرية، أبرزها:

- **تحقيق الشمول المالي:** من خلال تمكين شرائح واسعة من السكان من الوصول إلى الخدمات البنكية عبر الوسائط الرقمية، خاصة في المناطق النائية التي تفتقر إلى البنى التحتية البنكية.[2]
- **رفع جودة الخدمات المصرفية:** وذلك عبر توسيع نطاق الخدمات المقدمة، وسرعة تنفيذ المعاملات، وتقليل الأخطاء البشرية.
- **دعم الابتكار المالي:** مثل إدخال خدمات جديدة كالدفع الإلكتروني، والمحافظ الرقمية، وخدمات القروض عبر الإنترنت.
- **تعزيز قدرة البنك على تحليل البيانات:** إذ تتيح الحلول الرقمية إمكانيات تحليل متقدمة لسلوك العملاء، مما يسمح بتصميم منتجات وخدمات مخصصة بدقة.[3]
- **تعزيز الشفافية والرقابة:** تُمكّن البنوك من تتبع المعاملات بدقة عالية، مما يُسهم في مكافحة الفساد وتبييض الأموال.[4]

ويعد التحول الرقمي أداة جوهرية في الانتقال نحو نموذج بنكي أكثر ديناميكية وتكيفًا مع متغيرات السوق، **"التحول الرقمي يمثل خيارًا استراتيجيًا لا غنى عنه للبنوك الجزائرية لتحقيق استدامة تنافسية في البيئة الرقمية الجديدة"**[5]

الفرع الثالث: معوقات التحول الرقمي في البيئة المصرفية الجزائرية

رغم ما يتيحه التحول الرقمي من فرص للنهوض بالقطاع المصرفي الجزائري، إلا أنّ هذا المسار يواجه جملة من المعوقات البنيوية والتقنية والتنظيمية، التي تعرقل تنفيذ استراتيجيات رقمية فعالة وشاملة. وتتعدد هذه المعوقات لتشمل جوانب مرتبطة بالبنية التحتية، بالكفاءات البشرية، بالجانب القانوني، وبالثقافة التنظيمية والمالية.

---

[1] حمدي بن عاشور، "**أمن المعلومات كركيزة للتحول الرقمي في البنوك**"، مجلة الاقتصاد الجديد، العدد 15، 2021، ص. 89.

[2] دراسة بعنوان: "دور الرقمنة في تعميم الشمول المالي بالجزائر"، المركز الجامعي النعامة، 2022، ص. 51.

[3] OECD, Digital Transformation in Financial Services, 2021, p. 29.

[4] نفس المرجع السابق، ص. 30.

[5] بوزادية جمال، مرجع سابق، ص. 16.

-أولاً: ضعف البنية التحتية التكنولوجية : تعد البنية التحتية الرقمية حجر الأساس في أي تحول رقمي، غير أن العديد من البنوك الجزائرية لا تزال تعتمد على أنظمة قديمة ومتشظية، تفتقر إلى التكامل والأمان الكافي، ما يجعلها عاجزة عن استيعاب التطبيقات الرقمية الحديثة. كما تشير دراسة جزائرية إلى أن "الافتقار إلى منصات رقمية موحدة وآمنة يشكل أحد أبرز العوائق في وجه رقمنة الخدمات البنكية".[1]

-ثانياً: محدودية الكفاءات البشرية المتخصصة : تشير مذكرات أكاديمية إلى أنّ المؤسسات البنكية تعاني من نقص في المهارات الرقمية المتخصصة، خصوصًا في مجالات تحليل البيانات، وأمن المعلومات، وتطوير البرمجيات البنكية[2]. ويؤدي هذا النقص إلى إبطاء عملية تبني الحلول الرقمية أو تنفيذها بجودة متدنية.

-ثالثاً: تأخر الإصلاح القانوني والتشريعي : تتطلب البيئة الرقمية أطرًا قانونية مرنة تحكم التعاملات الإلكترونية وتضمن حماية المستهلك الرقمي، لكن الإطار القانوني في الجزائر لا يزال متأخرًا نسبيًا، ولا يغطي كافة أوجه المعاملات البنكية الرقمية[3]، كما أن غياب قانون موحد لحماية البيانات الشخصية يعرقل ثقة العملاء في استخدام الخدمات الرقمية.[4]

-رابعاً: ضعف الوعي الرقمي لدى الزبائن : تمثل الثقافة المصرفية الرقمية للمواطنين أحد التحديات الجوهرية، إذ لا تزال نسبة كبيرة من العملاء تفضل المعاملات التقليدية، إما لغياب الثقة في الوسائل الرقمية، أو لضعف المعرفة باستخدام التطبيقات البنكية الحديثة.[5]

-خامساً: نقص التمويل والاستثمار في الرقمنة : تتطلب مشاريع التحول الرقمي استثمارات ضخمة في البنية التحتية، والبرمجيات، وتدريب الموارد البشرية، وهو ما لا يتوفر بسهولة لكافة البنوك، خاصة البنوك العمومية ذات الطابع التقليدي، ما يؤدي إلى بطء في الانتقال نحو النموذج الرقمي.[6]

---

[1] بن عيسى سميرة، "**التحول الرقمي في البنوك الجزائرية كآلية لتحسين جودة الخدمة المصرفية**"، مذكرة ماجستير، جامعة البليدة 2، 2020، ص. 49.

[2] بوزادية جمال، "**فاعلية استراتيجيات الأمن السيبراني في البنوك الجزائرية**"، مذكرة ماجستير، كلية العلوم الاقتصادية، جامعة الجزائر 3، 2021، ص. 15.

[3] غربي علي، "**التحول الرقمي في المؤسسات الجزائرية: الواقع والتحديات**"، مجلة أبحاث اقتصادية، العدد 11، 2021، ص. 67.

[4] نفس المرجع السابق، ص. 70.

[5] بوزادية جمال، مرجع سابق، ص. 16

[6] جودي محمد، "**محددات تبني الرقمنة في البنوك الجزائرية**"، مجلة الاقتصاد الجديد، العدد 18، 2022، ص. 94.

–سادساً: ضعف التعاون بين البنوك وشركات التكنولوجيا المالية(Fintech) : يبقى التعاون بين القطاع المصرفي والمؤسسات الناشئة في مجال التكنولوجيا المالية ضعيفًا، ما يحرم البنوك من فرص الابتكار والتطوير المشترك[1].

وتجدر الإشارة إلى أن دراسة صادرة عن كلية العلوم الاقتصادية بجامعة الجزائر 3 تؤكد أن "نجاح التحول الرقمي في البيئة المصرفية الجزائرية يظل رهينًا بإصلاحات هيكلية عميقة على مستوى البنية القانونية والتقنية والتنظيمية، إضافة إلى تطوير الرأسمال البشري والوعي المجتمعي"[2].

المطلب الثالث: العلاقة بين إدارة المخاطر السيبرانية والتحول الرقمي

في ظل التحول الرقمي المتسارع الذي تشهده البنوك الجزائرية، أصبحت العلاقة بين إدارة المخاطر السيبرانية والرقمنة علاقة تكاملية لا غنى عنها. فبينما تسعى البنوك إلى تحسين خدماتها وتعزيز كفاءتها من خلال اعتماد الأنظمة الرقمية، تزداد في المقابل درجة تعرضها للمخاطر السيبرانية، الأمر الذي يجعل من الضروري وجود إستراتيجيات أمنية فعّالة ومتطورة لحماية الأصول الرقمية وضمان استمرارية العمليات المصرفية.

إن إدارة المخاطر السيبرانية لم تعد مسألة تقنية فقط، بل أصبحت ركيزة أساسية لضمان نجاح مشاريع التحول الرقمي، حيث يعتمد مدى فعالية الرقمنة على قدرة المؤسسات المصرفية على توقع التهديدات الإلكترونية، ومواجهتها ضمن إطار متكامل من الحوكمة الإلكترونية والتخطيط الاستراتيجي

الفرع الأول: التفاعل البنيوي بين الرقمنة والمخاطر السيبرانية في البيئة المصرفية

يُشير التفاعل البنيوي بين التحول الرقمي والمخاطر السيبرانية إلى العلاقة المركّبة التي تنشأ عند اعتماد التكنولوجيا الرقمية بشكل واسع داخل البنوك، مما يفتح المجال أمام تهديدات سيبرانية متطورة تستهدف البنية التحتية الرقمية والمؤسساتية لهذه البنوك. فالرقمنة، وإن كانت أداة لتعزيز الكفاءة، وتوسيع الشمول المالي، وتسهيل المعاملات المصرفية، فإنها في ذات الوقت توسّع ما يُعرف بـ"سطح الهجوم السيبراني(Attack Surface) "، وتفرض على البنوك تحديات أمنية غير تقليدية.[3]

إن البنوك الجزائرية التي تبنّت منظومات إلكترونية كجزء من عملية التحديث التكنولوجي وجدت نفسها أمام واقع يفرض ضرورة إعادة هيكلة أنظمتها الأمنية، حيث باتت المخاطر السيبرانية تشكل تهديدًا مباشراً لسلامة

[1] جودي محمد مرجع السابق، ص. 95.

[2] بوزادية جمال، مرجع سابق، ص. 17.

[3] سفيان عشي، "**أثر التحول الرقمي على أداء البنوك التجارية الجزائرية**"، مذكرة ماجستير، 2022، ص. 40.

العمليات المصرفية وسرية بيانات العملاء[1]. وقد أشار بوزيد سامي في دراسته حول الرقمنة في القطاع المصرفي إلى أن "كل خطوة نحو الرقمنة لا بد أن تقابلها خطوة مقابلة في اتجاه تأمين هذه الرقمنة" [2], ومن الناحية البنيوية، فإن كل عنصر من عناصر البنية التحتية الرقمية – كالشبكات، أنظمة المعالجة، قواعد البيانات، والتطبيقات المصرفية – يُعدّ نقطة اتصال محتملة مع البيئة الخارجية، وبالتالي مدخلاً محتملاً للهجمات السيبرانية. وهذا ما يجعل العلاقة بين الرقمنة والمخاطر السيبرانية علاقة جدلية؛ فكلما توسعت رقعة التحول الرقمي، ارتفعت معها الحاجة إلى ضوابط أمنية متكاملة.[3]

إن ضعف بعض البنوك الجزائرية في تبني حلول أمن سيبراني موازية لرقمنتها، يرجع إلى غياب ثقافة أمنية رقمية مؤسساتية، ونقص الاستثمار في الكفاءات المتخصصة، مما جعل من الرقمنة عاملاً محفزًا لظهور ثغرات إلكترونية خطيرة[4], وعليه، فإن العلاقة البنيوية بين الرقمنة والمخاطر السيبرانية في البيئة المصرفية ليست مجرد علاقة سببية، بل علاقة تداخل عضوي تفرض على الإدارات البنكية التفكير في الأمن السيبراني بوصفه جزءًا لا يتجزأ من هندسة الرقمنة ذاتها، وليس كخيار ثانوي أو ترف تقني.

الفرع الثاني: تأثير إدارة المخاطر السيبرانية على نجاح مشاريع التحول الرقمي

تعد إدارة المخاطر السيبرانية من المرتكزات الأساسية التي تضمن استمرارية ونجاح مشاريع التحول الرقمي في القطاع المصرفي، إذ إن التكنولوجيا الرقمية – رغم ما تحمله من فرص – تفتح الباب أمام تهديدات متعددة، ما لم تتم مواجهتها بخطط وقائية واستباقية دقيقة. إن تجاهل هذه المخاطر أو التقليل من شأنها قد يؤدي إلى فشل ذريع في تطبيق استراتيجيات التحول الرقمي، أو على الأقل إلى تعطيلها[5] , وقد بيّن سفيان عشي في دراسته أن غياب إدارة فعالة للمخاطر السيبرانية قد يؤدي إلى فقدان ثقة الزبائن في القنوات الرقمية، خاصة إذا ما ارتبطت بأحداث اختراق أو تسريب بيانات، مما يؤثر سلبًا على قابلية المستخدمين لتبنّي هذه الأنظمة[6]. وهو ما يجعل المؤسسات المصرفية تدرك أن التحول الرقمي لا يمكن أن يتحقق بمعزل عن البنية الأمنية المواكبة له، فنجاح مشروع رقمي ما لا يُقاس فقط بمدى جاهزيته التقنية، بل أيضًا بمدى قدرته على الصمود في وجه التهديدات الرقمية.

---

[1] سامي بن يحي، "**تحليل واقع المخاطر السيبرانية في البنوك العمومية الجزائرية**"، مذكرة ماجستير، 2021، ص. 34.

[2] بوزيد سامي، "**الرقمنة في القطاع المصرفي وأثرها على الشمول المالي**"، مذكرة ماجستير، 2022، ص. 58.

[3] نفس المرجع السابق، ص. 59.

[4] مونية بوشيخي، "**دور الرقمنة في تعميم الشمول المالي بالجزائر**"، مذكرة ماجستير، 2022، ص. 51.

[5] بوزيد سامي، "**الرقمنة في القطاع المصرفي وأثرها على الشمول المالي**"، مذكرة ماجستير، 2022، ص. 61.

[6] سفيان عشي، "**أثر التحول الرقمي على أداء البنوك التجارية الجزائرية**"، مذكرة ماجستير، 2022، ص. 41.

وفي هذا السياق، أشارت بوزيد سامي إلى أن بعض البنوك الجزائرية التي قامت بإطلاق منصات رقمية دون خطة أمنية محكمة تعرضت لصعوبات تقنية وتسريبات محتملة، مما دفعها إلى مراجعة بنيتها التحتية لاحقًا، وتخصيص ميزانيات إضافية لأمن المعلومات[1] , كما ذات المصدر أن العلاقة بين إدارة المخاطر السيبرانية ومشاريع الرقمنة هي علاقة تأثير مباشر، حيث أن وجود إدارة فعالة لتلك المخاطر يسهم في خلق بيئة مؤسسية آمنة تعزز الابتكار وتحفّز التحول الرقمي، في حين أن انعدامها يقود إلى مقاومة داخلية وخارجية للرقمنة بسبب الخوف من الهجمات الإلكترونية[2].

إن نجاح مشاريع التحول الرقمي في البنوك الجزائرية لا يكتمل إلا بتبنّي نهج شامل لإدارة المخاطر السيبرانية، يُدمج فيه البعد الأمني ضمن مراحل التخطيط والتنفيذ والتقييم لتلك المشاريع، وليس فقط كردّ فعل لاحق للتهديدات، مما يعكس نضجًا مؤسساتيًا حقيقيًا تجاه الرقمنة المستدامة.

الفرع الثالث: نحو تكامل استراتيجي بين الأمن السيبراني والتحول الرقمي في البنوك الجزائرية

يشهد القطاع المصرفي في الجزائر تحولات متسارعة نحو الرقمنة، غير أن هذا التوجه، إذا لم يُقرن بمنظور استراتيجي شامل للأمن السيبراني، قد يُفضي إلى اختلالات عميقة تُعيق فعالية هذه النقلة. إن التكامل بين التحول الرقمي والأمن السيبراني لا يجب أن يكون خيارًا تقنيًا لاحقًا، بل ضرورة استراتيجية مبدئية تُدمج ضمن الرؤية العامة للمؤسسات المالية منذ مرحلة التخطيط الأولى[3].

وقد أبرزت سامية لخضاري في دراستها أن البنوك الجزائرية تواجه تحديًا في تحقيق هذا التكامل، نظرًا لضعف التنسيق المؤسسي بين إدارات تكنولوجيا المعلومات ووحدات إدارة المخاطر، إضافة إلى غياب سياسات موحدة تستند إلى مبدأ أمن المعلومات أولاً[4]. فالتحول الرقمي قد يُسفر عن تعقيدات هيكلية جديدة تتطلب إعادة بناء منظومة الحوكمة بشكل يستوعب المتغيرات التكنولوجية ويضمن الأمان السيبراني كأولوية.

ومن جهة أخرى، ترى مروى بوعلي أن نجاح التحول الرقمي يتطلب ليس فقط تحديث البنية التحتية الرقمية، وإنما أيضًا إدماج الأمن السيبراني في كل مستويات العمل المصرفي، من تدريب الموظفين على الوعي الأمني، إلى تطوير

[1] نفس المرجع السابق، ص. 42.

[2] مونية بوشيخي، المرجع السابق ص. 53.

[3] سامية لخضاري، "**تحليل واقع الأمن السيبراني في البنوك الجزائرية**"، مذكرة ماجستير، جامعة قسنطينة 2، 2021، ص. 55.

[4] سامية لخضاري المرجع السابق، ص. 57.

بروتوكولات ذكية لرصد التهديدات والتحكم بها[1]. أي أن التكامل المقصود لا يكون على المستوى التكنولوجي فقط، بل كذلك على المستويين التنظيمي والثقافي داخل المؤسسة المصرفية.

إن التوجه نحو هذا النوع من التكامل يقتضي وضع خارطة طريق وطنية تشجع البنوك على تنسيق سياساتها الرقمية مع المعايير الدولية لأمن المعلومات، وتشجيع الابتكار في مجال التكنولوجيا المالية الآمنة (Secure FinTech). ولعل التجارب المقارنة لبعض الدول العربية، كما أشار فؤاد بومدين، تظهر أن البنوك التي دمجت الأمن السيبراني كركيزة استراتيجية في مشاريعها الرقمية، استطاعت رفع معدلات الاستخدام الرقمي، وزيادة ثقة الزبائن[2] , ومن ثمّ، فإن البنوك الجزائرية مطالَبة اليوم باعتماد مقاربة تكاملية متدرجة بين الأمن السيبراني والتحول الرقمي، تقوم على هندسة مؤسساتية مرنة، وبنية قانونية داعمة، ومورد بشري مؤهل، من أجل ضمان استدامة الابتكار المالي في بيئة أكثر أمانًا وكفاءة و ذلك ما يتضح من خلال هذا البحث .

إن العلاقة بين إدارة المخاطر السيبرانية والتحول الرقمي في البيئة المصرفية الجزائرية علاقة تكاملية تتطلب إدماجًا واعيًا ومتدرجًا بين مقاربتين استراتيجيتين متلازمتين. إذ لا يمكن إنجاح مشاريع الرقمنة دون بنية أمنية متينة، كما أن فعالية الأمن السيبراني رهينة بمدى مرونته وارتباطه بتطورات البنية التكنولوجية. ومن ثمّ، فإن بناء نموذج مصرفي عصري وآمن في الجزائر يقتضي تجاوز المقاربات التجزيئية، واعتماد رؤى شاملة تستوعب متطلبات الرقمنة من جهة، وضرورات الحماية المعلوماتية من جهة أخرى، ضمن أطر مؤسساتية وتشريعية متكاملة.

المبحث الثاني: الدراسات السابقة

يسعى هذا المبحث إلى تقديم نظرة تحليلية على الدراسات التي تناولت الأمن السيبراني والتحول الرقمي في البيئة البنكية، بتركيز خاص على البحوث المنجزة في الجزائر. الهدف هو تحديد مستويات المعرفة، واستخلاص الفجوات التي تسعى دراستنا الحالية لسدّها، بما يدعم رفع المساهمة العلمية للمنهج المقترح.

المطلب الأول : الدراسات على المستوى العالمي

الدراسة الأولى : أعدّ هذه الدراسة الباحث Richard Baskerville بعنوان "Cybersecurity Risk Management: A Review of Approaches and Challenges". نُشرت في مجلة Information Systems Management سنة 2018.

[1] مروى بوعلي، "**التحول الرقمي كخيار استراتيجي للبنوك الجزائرية: دراسة حالة بنك التنمية المحلية**"، مذكرة ماجستير، جامعة ورقلة، 2022، ص. 63.

[2] فؤاد بومدين، "**التحديات الأمنية في عصر الرقمنة المصرفية: دراسة مقارنة عربية**"، مذكرة ماجستير، جامعة البليدة 2، 2021، ص. 49.

تهدف الدراسة إلى تقديم مراجعة شاملة لمناهج إدارة المخاطر السيبرانية في بيئة الأعمال الحديثة، مع التركيز على المؤسسات المالية. بيّنت أن معظم البنوك تعتمد استراتيجيات تقنية بحتة في التصدي للهجمات، لكنها تهمل الأبعاد السلوكية والتنظيمية التي تعتبر حاسمة في بناء ثقافة أمنية مؤسسية. وأوصى الباحث بتبني نماذج هجينة تشمل التدريب، الرقابة، والمساءلة، إلى جانب الأدوات التكنولوجية.

الدراسة الثانية : قدّم الباحث Peter Bloxham دراسة بعنوان "Digital Transformation in Financial Services: The Role of Cyber Risk Management". نُشرت ضمن أبحاث The London Institute of Banking & Finance سنة 2020.

تناولت الدراسة العلاقة بين التحول الرقمي في البنوك وتزايد المخاطر السيبرانية. ركزت على البنوك الأوروبية كنموذج، موضحة كيف أن تسريع الرقمنة بسبب التنافس وتغير سلوك الزبائن قد فاقم من مستوى الهجمات السيبرانية. أوصى الباحث بوضع إدارة المخاطر السيبرانية ضمن التخطيط الاستراتيجي لرقمنة البنوك، وتحديث أنظمة المراقبة وتحليل التهديدات في الزمن الحقيقي.

الدراسة الثالثة : أنجزها الباحثان David W. Opderbeck & Orin S. Kerr بعنوان "The Law of Cybersecurity and the Financial Sector". نُشرت سنة 2021 في The Journal of Financial Regulation.

ركزت هذه الدراسة على الإطار القانوني والتنظيمي للأمن السيبراني في القطاع المصرفي الأمريكي، وبينت التحديات القانونية في التوفيق بين حماية البيانات وحق الزبون في الخصوصية. كما ناقشت كيفية تعامل البنوك مع القوانين الفيدرالية، وتقييم مدى كفايتها في صد التهديدات الرقمية. خلصت الدراسة إلى ضرورة تحديث التشريعات باستمرار وتبني مقاربة تشاركية بين البنوك والهيئات التنظيمية.

المطلب الثاني : الدراسات على مستوى الصعيد العربي

الدراسة الأولى: أعدّت هذه الدراسة الباحثتان سناء راهب وحليمة شابي, بعنوان: *"أثر التحول الرقمي على الأداء الوظيفي في البنوك التجارية الجزائرية – دراسة ميدانية على بعض البنوك بولاية الطارف"*، وهي مذكرة ماستر نوقشت بكلية العلوم الاقتصادية والتجارية وعلوم التسيير بجامعة الطارف سنة 2023.

هدفت الدراسة إلى تحليل العلاقة بين تطبيقات التحول الرقمي من جهة، ومستوى الأداء الوظيفي داخل البنوك الجزائرية من جهة أخرى. وركزت بشكل خاص على عناصر مثل استخدام البرمجيات الحديثة، وأتمتة المعاملات، والربط الشبكي بين الإدارات. وقد خلصت الدراسة إلى أن التحول الرقمي ساهم في تحسين الأداء من حيث

السرعة، وتقليل نسبة الأخطاء، ورفع جودة الخدمات المقدّمة للعملاء، إلا أن ذلك يبقى مرهونا بمستوى تكوين الموارد البشرية وتوفر البنية التحتية الرقمية المناسبة.

الدراسة الثانية : قام بإعداد هذه الدراسة فريق بحث مكوّن من ملاك بن نعمية، إيمان بن بوزيد، ونعيمة دبابسة، بعنوان: *"التحول الرقمي الذكي في بنك الفلاحة والتنمية الريفية – دراسة حالة وكالة الوادي"*، وهي مذكرة تخرج نوقشت بجامعة الوادي سنة 2023.

ركزت الدراسة على مدى إدماج البنك لتقنيات الذكاء الاصطناعي وإنترنت الأشياء في تقديم خدماته المالية، ومدى جاهزية الوكالة محل الدراسة للتكيّف مع التحولات الرقمية الحديثة. توصلت الدراسة إلى أن الوكالة قطعت خطوات معتبرة في تبنّي التحول الذكي، خصوصا في مجالات تسيير الحسابات وتقديم القروض وخدمات الدفع الإلكترونية، إلا أن هناك تحديات تتعلق بانخفاض مستويات التكوين في المجال الرقمي لدى الإطارات البنكية، وغياب رؤية استراتيجية شاملة لرقمنة المؤسسة.

الدراسة الثالثة : أنجزت هذه الدراسة الباحثة حياة بن كينة ، تحت عنوان: *"دور التحول الرقمي في تحسين الأداء المالي في البنوك – دراسة حالة القرض الشعبي الجزائري"*، وهي مذكرة ماستر نوقشت بجامعة غرداية سنة 2024.

سعت الدراسة إلى رصد أثر الرقمنة البنكية على الأداء المالي، باستخدام مؤشرات كمية مثل معدل نمو الأرباح، وحجم العمليات الإلكترونية، ومؤشر رضا الزبائن. وقد تمحورت حول تجربة القرض الشعبي الجزائري في تبني أدوات التحول الرقمي مثل الخدمات المصرفية عبر الإنترنت، وتطبيقات الهاتف المحمول، والصرافات الذكية. وبيّنت النتائج أن هناك تحسنا ملحوظا في الأداء المالي نتيجة التوجه الرقمي، لا سيما من خلال تخفيض التكاليف التشغيلية وتوسيع قاعدة العملاء، مع ضرورة الاهتمام بجانب الأمان السيبراني لتعزيز الثقة في القنوات الرقمية.

المطلب الثالث : الدراسات على المستوى المحلي (دراسات جزائرية)

الدراسة الأولى : أنجز هذه الدراسة الطالب زروقي عبد الحفيظ، بعنوان: "تحليل واقع المخاطر السيبرانية في البنوك العمومية الجزائرية – دراسة ميدانية ببنك الفلاحة والتنمية الريفية"BADR ، وهي مذكرة ماستر نوقشت بكلية العلوم الاقتصادية، جامعة قاصدي مرباح – ورقلة سنة 2021.

هدفت الدراسة إلى تشخيص طبيعة التهديدات السيبرانية التي تواجه البنوك العمومية، مع التركيز على مدى استعداد بنك الفلاحة والتنمية الريفية للتعامل مع هذه التهديدات. بيّنت نتائج الدراسة أن البنك يعاني من ضعف نسبي في تطبيق معايير الحماية الإلكترونية، خاصة في جانب التكوين المتخصص للموظفين في أمن المعلومات،

رغم توفر بعض أدوات الحماية التقنية. وأوصى الباحث بأهمية تطوير إطار استراتيجي لإدارة المخاطر السيبرانية، وتكوين فرق مختصة في الأمن السيبراني البنكي.

الدراسة الثانية : أنجزت هذه الدراسة الطالبة سهيلة بركاني، تحت عنوان: "فاعلية استراتيجيات الأمن السيبراني في البنوك الجزائرية – دراسة حالة بنك التنمية المحلية"BDL ، وهي مذكرة ماستر من جامعة الجزائر 3، كلية العلوم الاقتصادية، سنة 2021.

ركزت الدراسة على تحليل الاستراتيجيات المعتمدة من طرف بنك التنمية المحلية في مواجهة المخاطر الإلكترونية، من خلال مراجعة السياسات الأمنية الداخلية، وطرق الكشف المبكر عن الهجمات، وآليات الاستجابة. خلصت الدراسة إلى وجود تطور تدريجي في وعي الإدارة بأهمية الأمن السيبراني، مع وجود نقص في التشريعات البنكية الرقمية، وضعف التنسيق مع السلطات الرقابية. وأوصت بتحديث أنظمة الحماية الإلكترونية بشكل دوري، وربطها بقاعدة وطنية لتحليل المخاطر.

الدراسة الثالثة : أعدّها الطالب ياسين عيساوي، بعنوان: "دور الرقمنة في تعميم الشمول المالي في الجزائر – دراسة حالة بنك السلام"، مذكرة ماستر نوقشت بالمركز الجامعي بالنعامة سنة 2022.

هدفت هذه الدراسة إلى تحليل مدى مساهمة الرقمنة البنكية في توسيع قاعدة الزبائن وتحقيق الإدماج المالي، خاصة في المناطق النائية. استعرض الباحث تجربة بنك السلام في تقديم خدمات مالية رقمية موجهة للزبائن غير المتعاملين سابقا مع البنوك، مثل القروض الرقمية، والحسابات الإلكترونية، وتطبيقات الدفع عبر الهاتف. وقد أظهرت النتائج أن الرقمنة كانت عاملاً فاعلاً في تحسين الشمول المالي، رغم استمرار عقبات كضعف التغطية الرقمية، ونقص الثقة في الوسائل الإلكترونية لدى بعض شرائح المجتمع.

المطلب الرابع: مقارنة الدراسة الحالية مع الدراسات السابقة

تكشف مقارنة الدراسة الحالية مع الدراسات السابقة العربية، الجزائرية، والأجنبية عن تقاطعات واختلافات مهمّة تسهم في إثراء الإطار النظري والميداني لموضوع إدارة المخاطر السيبرانية في البنوك الجزائرية في ظل التحول الرقمي ,و الجدول التالي يوضح أوجه التشابه والاختلاف مع الدراسة الحالية

جدول رقم (1-1) : مقارنة موجزة بين الدراسة الحالية وبعض الدراسات السابقة

عنوان الدراسة	أوجه التشابه والاختلاف مع الدراسة الحالية	أهم النتائج	المنهج المعتمد
رحاب مرعي (2021) – جامعة القاهرة أثر التحول الرقمي على جودة الخدمات المصرفية	تتقاطع مع دراستنا في إبراز أهمية الرقمنة لكنها لم تتناول الأمن السيبراني	الرقمنة رفعت من كفاءة البنوك وأداء الخدمات	**وصفي تحليلي**
سعاد عرفة (2020) – جامعة دمشق التحديات الأمنية للتحول الرقمي في المؤسسات المالية	تتلاقى مع دراستنا في المخاطر الأمنية، لكنها ركزت على البيئة التشريعية	وجود ضعف تشريعي وأمني يهدد أمن البيانات الرقمية	**دراسة حالة**
نور خليل (2022) – الجامعة الأردنية الأمن السيبراني كمدخل استراتيجي لحماية نظم الدفع الإلكترونية	تشابه كبير في البعد الأمني، بينما دراستنا أوسع من حيث البنوك والتحول الرقمي	السياسات الأمنية تؤثر بفاعلية على حماية نظم الدفع	**تحليل وصفي**
سليماني عبد القادر (2021) – جامعة ورقلة تحليل واقع المخاطر السيبرانية في البنوك العمومية الجزائرية	تتفق مع دراستنا في طبيعة التهديدات، لكن دراستنا توسع الربط بالتحول الرقمي	أبرز التهديدات في ضعف التجهيزات والكوادر	**وصفي تحليلي**
زروقي فاطمة الزهراء (2021) – جامعة الجزائر 3فاعلية استراتيجيات الأمن السيبراني في البنوك الجزائرية	تتشابه مع دراستنا في النتائج، إلا أن دراستنا أعمق في الأبعاد الرقمية	أهمية تفعيل الحوكمة والرقابة الداخلية لتعزيز الأمن	**منهج وصفي تحليلي**
بوضياف نسرين (2022) – المركز الجامعي النعامة دور الرقمنة في تعميم الشمول المالي بالجزائر	تختلف في الهدف لكنها تلتقي معنا في رصد مزايا الرقمنة	الرقمنة وسعت قاعدة العملاء ودعمت الشمول المالي	**دراسة تحليلية**
Baskerville, R. (2018) – University of Auckland Cyber Risk Management in Digital Finance	دراسته مفاهيمية مقارنةً بدراستنا التطبيقية ضمن السياق الجزائري	يقدم نموذجًا تكامليًا لإدارة المخاطر في بيئة رقمية	**نظري استعراضي**
Kassem, H. (2019) – Oxford University Digital Transformation and Risk Exposure in Banking	تتلاقى مع دراستنا في الفكرة المركزية مع اختلاف في نطاق الدراسة	التحول الرقمي يرفع من فرص النجاح لكنه يزيد من المخاطر السيبرانية	**تحليل مقارن**
Lee, S. (2020) – Harvard Business School The Strategic Role of Cybersecurity in Banking Digitization	دراسته متقدمة في الطرح الفني، بينما دراستنا تركز على السياق الجزائري والعوامل المحلية	الأمن السيبراني ركيزة لنجاح التحول الرقمي المستدام	**تجريبية ميدانية**

المصدر : من اعداد الطالبتين بالاعتماد على بيانات الدراسة

فمن حيث المنهج , تشترك معظم الدراسات السابقة مع هذه الدراسة في اعتمادها على المنهج الوصفي التحليلي، غير أن بعض الدراسات الأجنبية – كدراسة – (2018) *Baskerville* سلكت منحى نظرياً استعراضياً متقدماً عبر تقديم مراجعات نقدية للمقاربات السائدة في إدارة المخاطر. أما الدراسة الحالية فقد أولت اهتمامًا خاصًا بجانب التفاعل البنيوي بين الرقمنة والمخاطر السيبرانية في السياق المحلي الجزائري، وهو ما لا نجده مفصلاً بنفس الشكل في الدراسات السابقة.

أما من حيث المجال المكاني والزماني , فتتميّز هذه الدراسة بتركيزها على البيئة الجزائرية في مرحلة حساسة من التحول الرقمي المصرفي (2020–2024)، وهو ما يمنحها بعدًا راهنيًا وميدانيًا مقارنة بدراسات عربية أو أجنبية ركّزت على تجارب أخرى (كالأردن أو أوروبا الغربية) ذات بنى تحتية رقمية متقدمة نسبيًا.

وفيما يتعلّق بنتائج الدراسات , فقد بيّنت غالبية الدراسات العربية والجزائرية – كدراسة الطالب *سليماني عبد القادر (2021) من جامعة ورقلة – بأن الخلل الأساسي في منظومة الأمن السيبراني بالبنوك الجزائرية يكمن في غياب استراتيجية وطنية موحدة للتعامل مع الهجمات الإلكترونية، إضافة إلى ضعف التكوين والتدريب. وقد دعمت الدراسة الحالية هذه الخلاصة، لكنها تجاوزت ذلك من خلال ربطها مباشرة بتأثير هذه التحديات على مشاريع التحول الرقمي البنكي، مبيّنة كيف تعرقل المخاطر السيبرانية إنجاح تلك المشاريع.

أما الدراسات الأجنبية، فقد ركزت – كما في دراسة – (2020) Bloxham على الجانب الاستراتيجي والتنظيمي للأمن السيبراني كأداة تمكينية للتحول الرقمي، وهو ما دفع هذه الدراسة إلى الدعوة لتبنّي مقاربة تكاملية بين الرقمنة وإدارة المخاطر بدل الفصل بينهما.

بوجه عام، تبيّن هذه المقارنة أن الدراسة الحالية تسهم في سد فجوة معرفية عبر تقديم قراءة مزدوجة للتفاعل بين الأمن السيبراني والتحول الرقمي في البيئة المصرفية الجزائرية، مقترحة تكاملاً استراتيجياً بعيدًا عن المعالجة التقنية البحتة التي غلبت على بعض الدراسات السابقة.

في ختام هذا المبحث، يتضح أن الدراسات السابقة، سواء العربية أو الجزائرية أو الأجنبية، قد تناولت موضوعي الأمن السيبراني والتحول الرقمي في القطاع المصرفي من زوايا متعددة، تراوحت بين التحليل النظري والدراسة التطبيقية، مع اختلاف في السياقات والبيئات التنظيمية. وقد أجمعت أغلبها على أن التحول الرقمي يشكل فرصة استراتيجية لتطوير الخدمات المالية، لكنه في الوقت ذاته يفتح المجال أمام مخاطر سيبرانية متزايدة تتطلب إدارة فعالة وتخطيطًا محكمًا. أما دراستنا الحالية، فتميزت بالربط العضوي بين هذين البعدين ضمن السياق الجزائري، مما يضفي عليها بعدًا تطبيقيًا ينسجم مع خصوصيات البيئة المصرفية المحلية، ويمنحها قيمة مضافة مقارنة بالدراسات السابقة.

خلاصة الفصل :

في ضوء ما تم تناوله في هذا الفصل النظري، تبيّن أن إدارة المخاطر السيبرانية والتحول الرقمي يشكلان ركيزتين أساسيتين في مستقبل العمل المصرفي، لاسيما في ظل التزايد المضطرد للاعتماد على التقنيات الحديثة. فقد تم توضيح الإطار المفاهيمي لإدارة المخاطر السيبرانية من حيث مفهومها، أنواعها، ومراحلها، مع التركيز على خصوصيات تطبيقها في البنوك الجزائرية، التي أصبحت معرّضة بشكل متزايد لهجمات إلكترونية تهدد استقرارها وسمعتها. كما تم التطرق إلى مفهوم التحول الرقمي، أبعاده، دوافعه، أهدافه، والمعوقات التي تواجه تطبيقه الفعلي في البيئة المصرفية الجزائرية، وذلك في ظل تحديات البنية التحتية والتأخر التشريعي والمؤسساتي.

وعبر ربط المكونين الأساسيين – الأمن السيبراني والتحول الرقمي – اتضح أن العلاقة بينهما تتسم بالتكامل والتفاعل، إذ لا يمكن إنجاح مشاريع الرقمنة دون تبني استراتيجيات صارمة وفعالة لإدارة المخاطر السيبرانية. وقد بيّن التحليل أن نجاح هذه العلاقة التكاملية يستوجب تبنّي مقاربات شاملة تشمل البعد التقني، التنظيمي، والبشري.

كما أبرز عرض الدراسات السابقة الأهمية الأكاديمية والعملية لهذا الموضوع، وساهم في الكشف عن الفجوات البحثية التي تسعى الدراسة الحالية إلى معالجتها، من خلال تقديم تصور متكامل حول واقع وتحديات إدارة المخاطر السيبرانية في ظل التحول الرقمي للبنوك الجزائرية.

الفصل الثاني :

الإطار التطبيقي للدراسة

تمهيد :

يأتي الفصل الثاني ليسلط الضوء على العلاقة بين التحول الرقمي – باعتباره متغيرًا مستقلًا – وبين إدارة المخاطر السيبرانية – بوصفها المتغير التابع – وذلك في سياق البنوك جزائرية تشهد تحولات متسارعة نحو الرقمنة. إذ يشكل هذا التحول الرقمي تحديًا مزدوجًا للبنوك العمومية، حيث يفرض عليها من جهة التكيّف مع مستجدات التكنولوجيا المالية، ومن جهة أخرى يُحمّلها مسؤوليات أمنية متزايدة لحماية نظمها ومعلوماتها من التهديدات السيبرانية.

كما يهدف هذا الفصل إلى تحليل طبيعة التهديدات السيبرانية التي تواجهها البنوك الجزائرية، واستكشاف مدى جهوزية فروع البنوك العمومية محل الدراسة (BEA – CPA – BNA) في مدينة ورقلة لمواجهتها، من خلال استعراض السياسات والآليات المعتمدة في إدارة هذه المخاطر. ومن خلال هذا التحليل، سيتم الوقوف على واقع تطبيق ممارسات الأمن السيبراني ومدى فاعليتها في ظل تبني تكنولوجيا التحول الرقمي، وذلك بغرض التمهيد للمعالجة الميدانية اللاحقة وتعزيز الإجابة على إشكالية الدراسة واختبار فرضياتها.

المبحث الأول: العينة وأدوات الدراسة

المطلب الأول: تحديد العينة وصفاتها

في سياق الدراسة التطبيقية لموضوع "إدارة المخاطر السيبرانية في البنوك الجزائرية في ظل التحول الرقمي: دراسة حالة لفروع البنوك العمومية بورقلة (BEA – CPA – BNA)"، تم اعتماد عينة قصدية من موظفي القطاع البنكي تم اختيارها بدقة، نظرًا لما يتطلبه موضوع الدراسة من فهم معمّق للإجراءات التقنية والتنظيمية المرتبطة بأمن المعلومات والتسيير الرقمي. وقد ركّزت المقابلات مع الإطارات المصرفية على الموظفين الذين يشغلون مناصب ذات صلة مباشرة بأنظمة الحماية الإلكترونية، الأمن السيبراني، الرقمنة، أو البنية التحتية التكنولوجية، وذلك بهدف تقييم مستوى الجاهزية والتحديات التي تواجهها البنوك العمومية في ورقلة في التصدي للمخاطر السيبرانية في ظل التحول الرقمي المتسارع.

الفرع الاول – نوع العينة

تم اعتماد عينة قصدية(Purposive Sample) ، وهي الأكثر ملاءمة لهذا النوع من الدراسات النوعية التحليلية، حيث تسمح بالتركيز على أفراد يملكون خبرة مباشرة في الموضوع المدروس. وقد تم اختيار هؤلاء الموظفين وفق معايير محددة تتعلق بمهامهم اليومية، ارتباطهم بمنظومة الرقمنة، ومسؤولياتهم في إدارة المعلومات أو تأمينها داخل المؤسسة.

الفرع الثاني – حجم العينة

بلغ حجم العينة ثمانية (8) موظفين موزعين على ثلاث مؤسسات بنكية عمومية، وفق التفصيل التالي:

- أربعة (4) موظفين من بنك – CPA الصندوق الشعبي الجزائري
- اثنان (2) من البنك الوطني الجزائريBNA
- اثنان (2) من بنك الجزائر الخارجيBEA

وقد تم اعتبار هذا الحجم كافيًا في إطار البحوث النوعية التي تركز على عمق المحتوى التحليلي أكثر من التمثيل الإحصائي، خصوصًا أن طبيعة الموضوع تتطلب استجواب أصحاب الخبرة والمعرفة التقنية المتخصصة.

الفرع الثالث– طريقة اختيار العينة

تم اختيار الأفراد بالتنسيق مع إدارات الموارد البشرية والفروع الجهوية للبنوك في ولاية ورقلة، حيث تم التركيز على الوظائف المرتبطة بـ:

- تسيير نظم المعلومات
- الأرشفة الرقمية
- خدمات الحماية السيبرانية
- التحول الرقمي البنكي

وتجدر الإشارة إلى أن بنك CPA هو الأكثر تعاونًا في توفير المعطيات التقنية الخاصة بالبنية الرقمية والأمن السيبراني، حيث قدّم مسؤولوه تسهيلات ملموسة في ما يخص المقابلات، وتوضيح الأنظمة المعتمدة، ومهام الموظفين، خلافًا للبنكين الآخرين اللذين عبّرا عن تحفظ نسبي في تقديم التفاصيل الدقيقة حول عدد الموظفين في الأمن السيبراني أو طبيعة عملهم.

الفرع الرابع – خصائص العينة

تمتاز العينة بخصائص وظيفية وتقنية متنوّعة، وهو ما يعكس تعددية وجهات النظر حول الإدارة الإلكترونية في السياق البنكي. ويمكن تلخيص الخصائص كما يلي:

الجدول رقم 2–1 : خصائص العينة

الخاصية	التوزيع
عدد الموظفين	**8موظفين**
المؤسسات	**CPA (4)، BNA (2)، BEA (2)**
الوظائف	**مسؤول نظم معلومات، تقني أرشفة، مختص أمن سيبراني، مهندس شبكات**
سنوات الخبرة	**تتراوح بين 5 و22 سنة**
المؤهل العلمي	**ليسانس/ماستر في الإعلام الآلي، الاقتصاد الرقمي، التسيير**
الموقع الجغرافي	**ولاية ورقلة**

المصدر : من اعداد الطالبتين بالاعتماد على بيانات الدراسة

كما أشار أحد الموظفين من بنك BEA إلى أن عدد موظفي الأمن السيبراني يبلغ ثمانية (8) داخل البنك على المستوى الوطني، في حين امتنعت المؤسستان الأخريان CPA) و (BNAعن الكشف عن عدد موظفي هذا التخصص بدقة لأسباب تتعلق بالسرية والخصوصية الأمنية.

إضافة إلى ذلك، فإن إدارة البنك الوطني الجزائري BNA كانت الوحيدة التي سمحت جزئيًا بالاطلاع على بعض تفاصيل الأنظمة المعتمدة مثلC6 ، C8، غير أن بنك CPA قدّم القدر الأكبر من المعلومات التفصيلية والمفيدة، مما جعله محورًا أساسًا في الجزء الميداني من الدراسة.

المطلب الثاني: أداة الدراسة – المقابلة كوسيلة لجمع البيانات

في إطار تنفيذ الدراسة التطبيقية حول "إدارة المخاطر السيبرانية في البنوك الجزائرية في ظل التحول الرقمي: دراسة حالة لفروع البنوك العمومية بورقلة (BEA – CPA – BNA)"، تم الاعتماد على المقابلة نصف الموجهة كأداة أساسية لجمع المعطيات، وذلك بالنظر إلى خصوصية الموضوع وحساسيته من جهة، واعتبارات البيئة البنكية من جهة أخرى، لا سيما ما يتعلق بأنظمة المعلومات، آليات الحماية، وتوزيع المهام ذات الصلة بالبنية التحتية الرقمية، وهو ما يتطلّب نقاشًا مفتوحًا مع المعنيين بالإدارة التقنية والمعلوماتية داخل الفروع المستهدفة.

–أولًا: أسباب اختيار أداة المقابلة

اعتمدت الباحثتان على أداة المقابلة بالنظر إلى:

- طبيعة الموضوع الذي يستلزم الوصول إلى مضامين غير منشورة أو غير متاحة للعامة، مثل تفاصيل أنظمة الحماية الرقمية والتطبيقات المستعملة في المعالجة الإلكترونية داخل البنوك.
- الحاجة إلى معطيات تفسيرية وتحليلية من داخل المؤسسات البنكية، خاصة تلك التي لا يمكن رصدها من خلال استبيانات أو تقارير منشورة.
- عدد الموظفي البنوك في هذا المجال قليل و لا يسمح بالاعتماد على الاستبيان
- رغبة الباحثتين في استكشاف مستوى التوظيف الفعلي لممارسات إدارة المخاطر السيبرانية في البنوك العمومية، وليس الاكتفاء بتحليل الأطر النظرية أو التصورات التنظيمية المعتمدة.

–ثانيًا: إعداد المقابلة وبناؤها

تم بناء المقابلة بالاعتماد على الأطر النظرية الحديثة ذات الصلة بالأمن السيبراني، والتحول الرقمي، وإدارة أمن المعلومات، وتم تنظيمها في ثلاثة محاور رئيسية، هي:

– المحور الأول: التحول الرقمي في البنوك العمومية

- يتناول هذا المحور مدى تبني البنوك لأنظمة رقمية متقدمة، ومستوى الاعتماد على الحلول الرقمية الذكية، وآليات رقمنة الخدمات البنكية الأساسية، مع التركيز على ما يرافق ذلك من متطلبات أمنية لحماية البيانات والمعاملات.

– المحور الثاني: الأمن السيبراني وحماية الأنظمة

- ويشمل أسئلة تتعلق بكفاءة أنظمة الحماية، عدد الموظفين المكلّفين بالأمن السيبراني، والبرمجيات المعتمدة، إضافة إلى مدى تعاون الإدارة في الكشف عن البنية الأمنية.

– المحور الثالث: تقييم فعالية الانظمة الرقمية من وجهة نظر الموظفين

- ويتناول الانطباعات حول فعالية الأنظمة الرقمية في تسهيل العمل، معالجة شكاوى الزبائن، ضمان استمرارية الخدمة، وتحقيق الكفاءة التشغيلية.

– ثالثا ; تنفيذ المقابلة ميدانيًا

تم إجراء المقابلات مع ثمانية موظفين موزعين كما يلي:

- أربعة موظفين من بنكCPA ، وهو البنك الذي قدم أكبر قدر من التعاون والمعلومات، خاصة فيما يخص الأنظمة المعتمدة، نوع البرمجيات، إجراءات الأمن، وتوزيع المهام الرقمية.
- موظفين من بنكBEA ، الذين أفادا بوجود ثمانية (8) موظفين على المستوى الوطني مختصين بالأمن السيبراني، لكنهما تحفظا على ذكر مزيد من التفاصيل التقنية حول أنواع الحماية.
- موظفين من بنكBNA ، الذي أكدا اعتماد البنك على بعض الأنظمة الإلكترونية مثل C6 وC8، في حين امتنعت الإدارة عن تقديم بيانات دقيقة حول عدد موظفي الأمن السيبراني أو نمط الحماية المعتمد.
- تم تسجيل الردود كتابيًا بعد أخذ الموافقة الشفوية من كل موظف، حيث رفض أغلبهم استخدام أجهزة التسجيل الصوتي نظرًا لحساسية المواضيع.

– رابعا ; مصداقية الأداة وضمان جودتها العلمية

صدق الأداة ; (**Credibility**) تحقق عبر التحكيم الأكاديمي للمقابلة، وتوظيف محاور واضحة تستهدف الجوانب الإدارية والتقنية الحقيقية في بيئة العمل البنكي.

ثبات الأداة ; (**Dependability**) تم ضمانه بتطبيق نفس دليل المقابلة مع جميع المشاركين، وتوثيق الردود بطريقة منظمة قابلة للمراجعة والتحليل.

المطلب الثالث: تحليل محتوى المقابلات وتصنيف المعطيات حسب المؤسسات والفئات

بُني هذا المطلب على تفريغ وتحليل محتوى المقابلات النوعية التي أُجريت مع عينة قصدية من موظفي ثلاث مؤسسات مصرفية جزائرية، هي: بنك التنمية المحلية(CPA) ، بنك الجزائر الخارجي(BEA) ، والبنك الوطني الجزائري .(BNA) وقد تم تحليل المعطيات وفق المحاور الرئيسة المعتمدة، وتصنيفها بحسب البنك ومجال الاختصاص، وذلك باستخدام أسلوب التحليل الموضوعي الذي يركز على المضامين المتكررة والدلالات التقنية.

- **أولًا ; توزيع المبحوثين حسب البنك والمجال التقني**

الجدول رقم 2-2 : توزيع المبحوثين حسب البنك والمجال التقني

البنك	عدد المبحوثين	الملاحظات الرئيسية	المجال الوظيفي
بنكCPA	4موظفين	قدموا أكبر حجم من المعطيات الدقيقة والعملية.	**مختصون في الأمن السيبراني وأنظمة الشبكات**
بنكBEA	2موظفين	تحفّظ جزئي في تقديم المعلومات الأمنية الحساسة.	**موظف تقني عام وآخر إداري**
بنكBNA	2موظفين	تعاون نسبي، دون تفصيل في طبيعة الأنظمة المستخدمة.	**مسؤول تقني وموظف إداري**

المصدر : من اعداد الطالبتين بالاعتماد على بيانات الدراسة

وقد بلغ العدد الإجمالي للمبحوثين 8 موظفين تمثلوا جميعًا في كوادر عاملة ضمن أقسام مرتبطة مباشرة أو غير مباشرة بالأمن السيبراني، والتحول الرقمي، مما وفّر قاعدة غنية للتحليل النوعي.

– ثانيًا; تحليل المحور الأول – واقع الإدارة الإلكترونية ; أكّد بنك CPA أن التحول الرقمي يشكل أحد محاور تحديث الخدمة العمومية المصرفية، حيث تم اعتماد منظومات إلكترونية لإدارة الوثائق والعمليات البنكية عن بُعد، ضمن بيئة معلوماتية مؤمنة نسبيًا. أما بنك BEA و :BNAعبّر الموظفون عن اعتماد تدريجي وبطيء للنظم الإلكترونية، مع بقاء بعض المسارات الورقية. وقد أشار أحد موظفي BNA إلى استخدام أنظمة تشغيل داخلية مثل C6 وC8، دون توضيح لمسارات الاستخدام.

– ثالثًا ; تحليل المحور الثاني ;– الأمن السيبراني وأنظمته أكد المشاركون أن الأمن السيبراني يُدار ضمن نطاق مركزي تحت إشراف بنك الجزائر، ويُزوَّد كل بنك بالبروتوكولات والسياسات العامة للحماية، فيما يخص أنظمة المراقبة، الكشف المبكر، والتفاعل مع التهديدات , وفي بنكCPA ، أشار الموظفون إلى وجود طاقم تقني متخصص مزوّد بأدوات مراقبة أمنية رقمية، مع تكوين دوري وتحديث للمنصات الرقمية، ما يعكس درجة احترافية أعلى مقارنة بالبنكين الآخرين , أما في BEA وBNA، فقد أبدى المشاركون تحفظًا كبيرًا على ذكر تفاصيل

تتعلق بتقنيات الحماية وأنواع البرمجيات، مبررين ذلك بخصوصية الملف الأمني الرقمي، واقتصار الإشراف عليه على الإدارة العليا والتنسيق مع الجهات السيادية.

–رابعًا ; تحليل المحور الثالث ;– جودة الخدمات الرقمية والتحديات الميدانية

اتفق موظفو بنك CPA على أن جودة الخدمات الرقمية تتفاوت باختلاف الفروع، وأن التحدي الأبرز يتمثل في ضعف التكوين الرقمي لدى بعض الموظفين، إضافة إلى محدودية الثقافة الإلكترونية لدى الزبائن.

في المقابل، لم يُقدّم موظفو BEA و BNAتقييماً تفصيليًا لجودة الخدمات، لكنهم أشاروا إلى عراقيل إدارية وتشغيلية تعيق التحول الرقمي الكامل، أبرزها البيروقراطية وضعف الدعم الفني.

– خامسًا ; ملاحظات منهجية وتحليلية

أظهرت المعطيات أن أغلب البيانات التقنية الغنية جاءت من بنكCPA ، حيث أبدت إدارته تعاونًا كبيرًا، مقارنة بـ BEA و BNAاللذَين اتّسما بالحذر في التصريح و رغم أن عدد موظفي الأمن السيبراني الكلي بلغ 8 موظفين، فإن التوزيع الداخلي يُظهر تمركز الخبرة بشكل واضح في 4 موظفين CPA ، مع تواجد محدود في BEAو 2) BNAلكل بنك)، مما قد يعكس تفاوتًا في الهيكلة التقنية والقدرات البشرية , أيضا وفّرت المقابلات بيئة خصبة لفهم الواقع السيبراني في القطاع المصرفي، خاصةً في ظل التفاوت بين البنوك في مستوى الانفتاح، ونوع الأنظمة المعتمدة، ومدى جاهزية البنية التحتية الرقمية.

المطلب الرابع: المنهج المستخدم في الدراسة

نظراً لطبيعة موضوع الدراسة الذي يتناول واقع وآليات الأمن السيبراني في البنوك العمومية الجزائرية، فقد تم الاعتماد على المنهج الوصفي التحليلي الكيفي Qualitative Descriptive-Analytical) (Method، والذي يُعدّ من أكثر المناهج ملاءمةً للبحوث التي تسعى إلى فهم الظواهر المعقدة من داخلها، واستكشاف تصورات الفاعلين وممارساتهم في السياق الطبيعي لها , وقد اعتمدت الباحثتان في تحليل البيانات المجمعة على أسلوب التحليل الموضوعي المحوري(Thematic Analysis) ، والذي يقوم على تصنيف البيانات وفق محاور رئيسة متكررة تم استخلاصها من أجوبة المستجوبين. وقد مكّن هذا الأسلوب من إبراز النقاط المشتركة والمختلفة بين البنوك الثلاثة، وفهم الممارسات التقنية والإدارية في مجال الأمن السيبراني، لا سيما بعد أن تبيّن أن بنك CPA كان الأكثر تعاوناً وتفصيلاً في تزويد الباحثتين بالمعلومات.

كما أن توزيع العينة ساعد على تغطية مختلف أوجه الظاهرة، حيث تم إجراء المقابلات مع 8 موظفين .

المبحث الثاني: عرض وتحليل ومناقشة نتائج الدراسة الميدانية

برزت أهمية إدارة المخاطر السيبرانية كأولوية استراتيجية، سيما في ظل محدودية الإمكانيات التقنية والبشرية، ونقص التأطير التنظيمي والتشريعي , ومن خلال هذا المبحث نسلط الضوء على واقع وآليات إدارة هذه المخاطر في البنوك العمومية بالجزائر، من خلال تحليل إجابات عينة ميدانية مكوّنة من 8 موظفين موزعين على فروع بنوك BEA وCPA وBNA بمدينة ورقلة. ويتضمن هذا المبحث عرضًا دقيقًا وتحليلاً مفصلاً للنتائج المجمعة حسب المحاور الأساسية، تليها مناقشة هذه النتائج في ضوء الفرضيات التي انطلقت منها الدراسة.

المطلب الأول: عرض وتحليل نتائج الدراسة حسب المحاور

المحور الأول: واقع المخاطر السيبرانية التي تواجه البنوك العمومية في ظل التحول الرقمي

يتناول هذا المحور مستوى ودرجة المخاطر السيبرانية التي تواجه البنوك العمومية نتيجة التحول الرقمي، من خلال إدراك المبحوثين لدرجة التهديدات، أنواع الهجمات المتكررة، والأقسام الأكثر عرضة لهذه التهديدات.

الجدول رقم 2-3 : تقييم مستوى المخاطر السيبرانية حسب آراء المبحوثين

البنك	عدد المبحوثين	ضعيف	متوسط	مرتفع
CPA	4	0	1	**3**
BEA	2	0	1	**1**
BNA	2	0	1	**1**
المجموع	**8**	**0**	**3**	**5**

المصدر : من اعداد الطالبتين بالاعتماد على بيانات الدراسة

تشير نتائج الجدول والشكل إلى أن غالبية المبحوثين (62.5%) يرون أن مستوى التهديدات السيبرانية التي تواجهها بنوكهم "مرتفع"، بينما يرى 37.5% أن هذه التهديدات في مستوى "متوسط"، ولم يُسجل أي تقييم بأنها "منخفضة". ويعكس هذا إدراكًا واضحًا لدى موظفي البنوك لأهمية الخطر السيبراني وتناميه في سياق التوسع في تقديم الخدمات المصرفية الإلكترونية.

كما يبرز من المعطيات أن التحول الرقمي في البنوك الجزائرية لم يكن مصحوبًا بنفس الدرجة من التحديث في أنظمة الحماية أو الاستعدادات التقنية. ويؤكد الموظفون أن أكثر أشكال التهديدات شيوعًا تشمل محاولات الاختراق، وهجمات الفدية(Ransomware) ، وتسريب البيانات.

هذه النتيجة تؤيد الفرضية الأولى من الدراسة، التي تفيد بأن البنوك الجزائرية تواجه مخاطر سيبرانية متزايدة بسبب التوسع في استخدام التكنولوجيات الرقمية.

الشكل رقم 2-1 : تقييم مستوى التهديدات السيبرانية

المحور الثاني: آليات إدارة المخاطر السيبرانية في البنوك العمومية

الجدول رقم 2-4 : الوسائل والآليات المعتمدة لإدارة المخاطر السيبرانية حسب آراء المبحوثين

نوع الوسيلة أو الآلية	عدد المبحوثين الذين أشاروا إليها	النسبة المئوية(%)
برامج الحماية(Antivirus / Firewall)	8	**100%**
أنظمة كشف التسلل(IDS/IPS)	4	**50%**
بروتوكولات التشفير	3	**37.5%**
تدريب المستخدمين وتوعيتهم	2	**25%**
خطة استجابة للحوادث السيبرانية	1	**12.5%**
تقييم دوري لمخاطر النظام المعلوماتي	2	**25%**
المجموع (عدد المبحوثين = 8)		

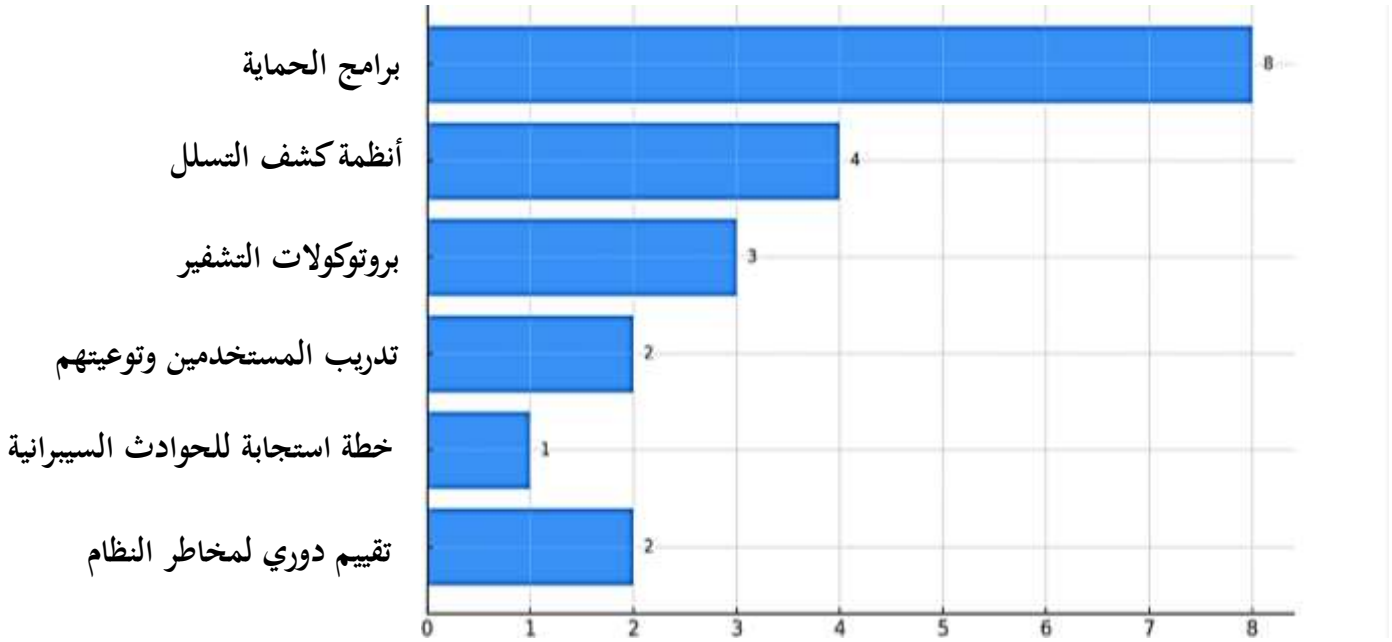
المصدر : من اعداد الطالبتين بالاعتماد على بيانات الدراسة

توضح نتائج الجدول والشكل أعلاه أن جميع البنوك محل الدراسة تعتمد على برامج الحماية الأساسية مثل مضادات الفيروسات والجدران النارية، مما يدل على الوعي العام بضرورة وجود طبقة أولية من الحماية. إلا أن الاعتماد على آليات أكثر تقدماً مثل أنظمة كشف التسلل أو بروتوكولات التشفير لا يزال محدودًا، حيث لم تتجاوز نسبة الذين أشاروا إلى استعمالها 50% و37.5% على التوالي.

أما التكوين والتدريب، وهو عنصر جوهري في تعزيز أمن النظام البشري داخل المؤسسة، فقد أشار إليه 25% فقط، ما يُظهر خللاً واضحًا في الاهتمام بالعنصر البشري ضمن سياسة الأمن السيبراني. كما أن إعداد خطط استجابة للحوادث لا يزال غائبًا تقريبًا، حيث لم يشر إليها سوى مبحوث واحد فقط (12.5%).

هذه النتائج تؤكد الفرضية الثانية من الدراسة، والتي نصت على أن البنوك الجزائرية تعتمد على مجموعة من الوسائل في إدارة المخاطر السيبرانية، إلا أنها تعاني من نقائص على مستوى الكفاءات البشرية، والجاهزية التقنية، وكفاءة أنظمة الحماية.

الشكل رقم2-2 : يوضح توزيع الوسائل والآليات المعتمدة لإدارة المخاطر السيبرانية من طرف الموظفين



المحور الثالث: الإطار التنظيمي والتكوين في الأمن السيبراني

يتعلق هذا المحور باستقصاء آراء المبحوثين حول العوائق التنظيمية والبشرية التي تؤثر على فعالية إدارة المخاطر السيبرانية، لا سيما مدى توفر الإطار القانوني والتشريعي، ومدى كفاءة التكوين المتخصص للموظفين في مجال الأمن السيبراني.

الجدول رقم 2–5: آراء المبحوثين حول العوائق التنظيمية والبشرية المرتبطة بإدارة المخاطر السيبرانية

رقم السؤال	المجموع الكلي (8)	المضمون	BNA (2)	BEA (2)	CPA (4)	المجموع الكلي (8)
1	نعم: 7 لا: 1	هل تعتقد أن غياب إطار تنظيمي واضح يمثل عائقاً في تطبيق سياسات الأمن السيبراني؟	نعم: 0 لا: 2	نعم: 0 لا: 2	نعم: 1 لا: 3	**نعم: 1 لا: 7**
2	نعم: 1 لا: 7	هل تتلقى تكويناً متخصصاً ومستمراً في الأمن السيبراني؟	نعم: 2 لا: 0	نعم: 2 لا: 0	نعم: 3 لا: 1	**نعم: 7 لا: 1**
3	نعم: 0 لا: 8	هل ترى أن التكوين الحالي كافٍ للتعامل مع التهديدات السيبرانية؟	نعم: 0 لا: 2	نعم: 0 لا: 2	نعم: 0 لا: 4	**نعم: 0 لا: 8**
4	نعم: 8 لا: 0	هل ترى ضرورة وضع إطار قانوني موحد خاص بإدارة الأمن السيبراني في البنوك الجزائرية؟	نعم: 0 لا: 2	نعم: 0 لا: 2	نعم: 0 لا: 4	**نعم: 8 لا: 0**

المصدر : من اعداد الطالبتين بالاعتماد على بيانات الدراسة

من خلال نتائج الجدول رقم (3) والشكل المصاحب له، يمكن استخلاص النقاط التالية:

غياب إطار تنظيمي واضح: 87.5%من المستجوبين (7 من أصل 8) أكدوا على أن غياب إطار قانوني وتشريعي واضح يُعد أحد أبرز العوائق أمام تطبيق سياسات فعّالة للأمن السيبراني.

يعكس هذا إجماعاً شبه تام على وجود فراغ تشريعي، حيث تعتمد البنوك حالياً على مذكرات داخلية أو تعليمات عامة غير مخصصة للأمن السيبراني.

التكوين المتخصص: أشار 87.5% من المبحوثين (7 من أصل 8) إلى عدم تلقيهم لأي تكوين متخصص ومستمر في مجال الأمن السيبراني، وهذا يمثل ضعفاً واضحاً في تنمية القدرات البشرية.

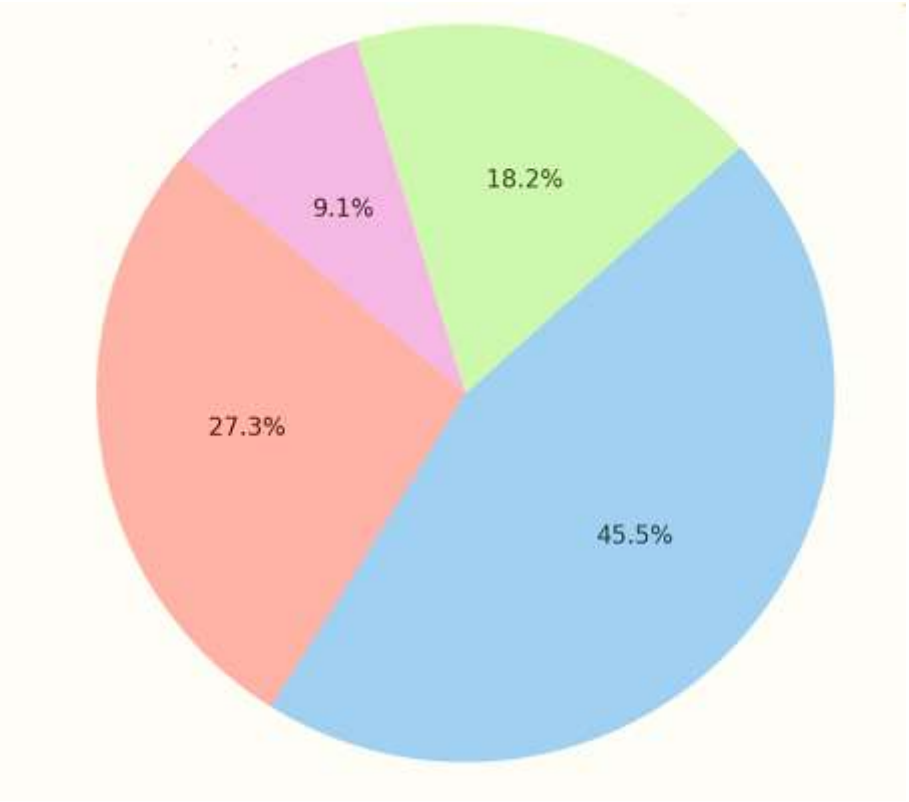
حتى المستجوب الوحيد الذي ذكر حصوله على تكوين، أوضح في التعليقات المرفقة أنه تكوين قصير المدى لا يرقى لمستوى التهديدات السيبرانية الحديثة.

عدم كفاية التكوين: جميع المبحوثين (100%) أجمعوا على أن التكوين المتاح لا يلبي الحاجيات الحقيقية لمواجهة التهديدات السيبرانية، ما يعزز فرضية أن غياب التكوين أحد عوامل ضعف الجاهزية المؤسسية.

الحاجة لإطار قانوني موحد: كل المستجوبين (8 من 8) أكدوا الحاجة إلى وجود إطار قانوني وتشريعي وطني موحد ينظم مجال الأمن السيبراني في القطاع البنكي، بما يشمل معايير الأمن، آليات الاستجابة، وتدابير الوقاية.

تكشف النتائج الخاصة بهذا المحور عن ضعف واضح في الجانب التنظيمي والتكويني داخل البنوك العمومية محل الدراسة، إذ إن غياب إطار قانوني منظم، وندرة التكوين المتخصص، يمثلان تحديين حقيقيين أمام تنفيذ سياسات فعالة في مجال الأمن السيبراني. وتتماشى هذه النتائج مع الفرضية الثالثة التي تفترض أن غياب الإطار التنظيمي ونقص التكوين المتخصص يمثلان أحد أبرز العوائق التي تحد من فعالية إدارة المخاطر السيبرانية.

الشكل رقم 2-3 : توزيع آراء المستجوبين حول العوائق التنظيمية والتكوينية في الأمن السيبراني



المحور الرابع: التكامل بين التحول الرقمي واستراتيجية الأمن السيبراني

يرتبط هذا المحور بتحليل إجابات المستجوبين حول مدى وجود تكامل فعلي بين جهود التحول الرقمي من جهة، واستراتيجية الأمن السيبراني من جهة أخرى، وهو ما يمثّل الأساس العملي للفرضية الرابعة.

جدول رقم 2–6 : آراء المستجوبين حول مدى التكامل بين التحول الرقمي واستراتيجية الأمن السيبراني

رقم المستجوب	البنك	هل يوجد تكامل حقيقي؟	توضيح الإجابة
1	CPA	نعم	**توجد استراتيجية أمن معلومات ترافق الرقمنة، خاصة في الخدمات عبر الإنترنت.**
2	CPA	لا	**المشاريع الرقمية تتقدم بسرعة لكن الأمن لا يواكبها بنفس المستوى.**
3	CPA	نسبيًا	**توجد محاولات، لكن غياب كفاءات داخلية متخصصة يضعف مستوى التكامل.**
4	CPA	نعم	**البنك يفرض التزامًا صارمًا بدمج الحماية المعلوماتية في كل مشروع رقمي جديد.**
5	BEA	لا	**لا توجد رؤية واضحة للأمن السيبراني داخل مشاريع التحول الرقمي.**
6	BEA	لا	**يتم اعتماد حلول جاهزة دون تقييم مخاطرها، الأمن غير مدمج استراتيجيًا.**
7	BNA	نسبيًا	**بعض المبادرات الرقمية تراعي الأمن، لكن لا توجد خطة موحدة.**
8	BNA	نعم	**استراتيجية الرقمنة مرتبطة بإجراءات وقائية للأمن السيبراني.**

المصدر : من اعداد الطالبتين بالاعتماد على بيانات الدراسة

أظهر التحليل النوعي لإجابات المستجوبين اختلافًا واضحًا في تقدير مستوى التكامل المؤسسي بين مشاريع التحول الرقمي في البنوك الجزائرية واستراتيجية الأمن السيبراني. وقد تباينت الآراء بين من يرى أن هناك ربطًا وتكاملاً فعليًا، خاصة لدى بعض فروع بنك CPA وBNA، وبين من يرى أن الأمن السيبراني لا يزال يُنظر إليه كـ"مكمّل لاحق" وليس كجزء مدمج في بنية النظام الرقمي.

ما يثير الانتباه أن 37.5% من المستجوبين أكدوا وجود تكامل فعلي، مقابل نفس النسبة التي نفت هذا التكامل بشكل قاطع، في حين أن 25% قدّرت أن الأمر لا يزال في طور المحاولة ولم يصل إلى مرحلة استراتيجية ناضجة. هذا التوزيع يعكس تباينًا مؤسسيًا في التعامل مع الأمن السيبراني، ويُظهر في الوقت ذاته أن بعض البنوك بدأت تستوعب أهمية الدمج المبكر للأمن المعلوماتي في كل مراحل تصميم الخدمات الرقمية.

بالمقابل، أشار بعض المستجوبين إلى أن بعض المشاريع الرقمية يتم تنفيذها بناءً على تعليمات من المركزية أو وفق برامج جاهزة تُطبّق دون تحليل للمخاطر أو مراجعة البنية التحتية الأمنية. هذا يشير إلى غياب تصور استراتيجي موحد داخل البنوك العمومية.

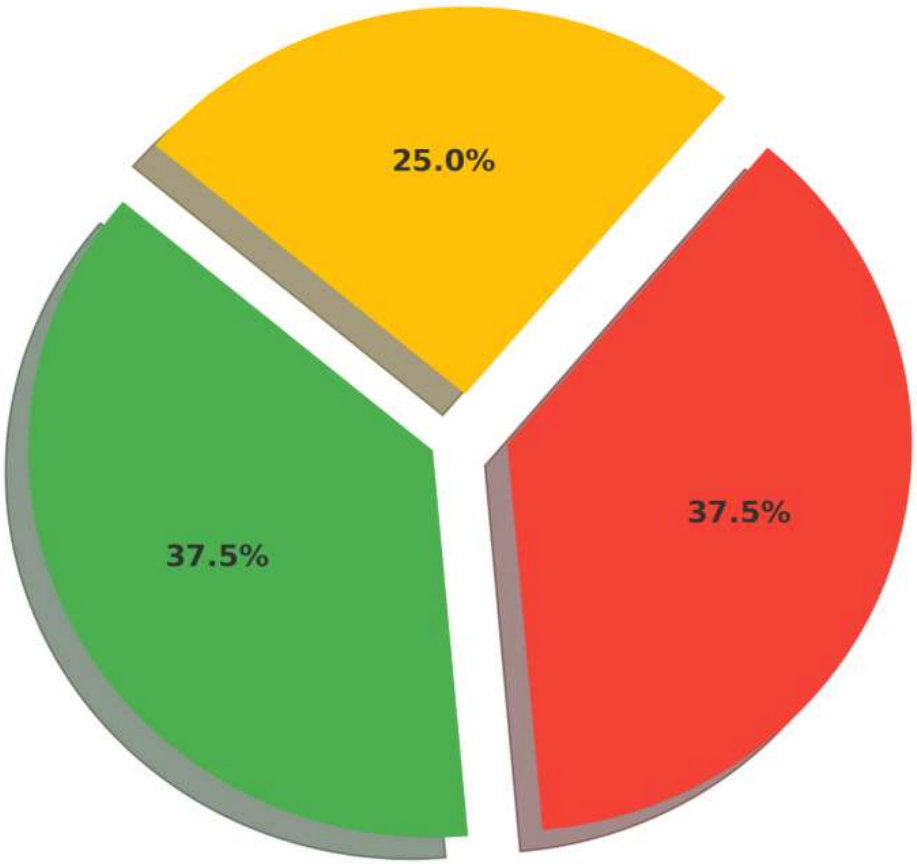
يتضح كذلك أن البنوك التي توفرت لديها لجان أمن معلومات أو هيئات إشراف داخلية كانت أكثر قدرة على تحقيق هذا التكامل. أما البنوك التي لا تمتلك هيكلة واضحة أو تفتقر إلى الكفاءات البشرية التقنية في هذا المجال، فقد جاء تقييمها سلبيًا أو ضعيفًا.

يدل تحليل هذا المحور على أن تحقيق التكامل بين الأمن السيبراني والتحول الرقمي ما يزال نسبيًا وغير موحد بين البنوك العمومية، رغم وجود بعض المبادرات الجادة في هذا المجال. وبهذا، فإن الفرضية الرابعة التي تقول إن:

"يُعتبر التكامل بين التحول الرقمي واستراتيجية الأمن السيبراني عنصرًا حاسمًا في تعزيز قدرة البنوك الجزائرية على مواجهة المخاطر السيبرانية، وذلك انطلاقًا مما تكشف عنه المعطيات الميدانية وآراء الفاعلين في القطاع البنكي".

تُعد فرضية مقبولة جزئيًا بناءً على آراء المستجوبين، مع التأكيد على ضرورة تعزيز هذا التكامل بمقاربة استراتيجية موحدة على المستوى الوطني والمؤسساتي.

الشكل رقم 2-4: توزيع آراء المستجوبين حول مستوى التكامل بين التحول الرقمي والأمن السيبراني



المطلب الثاني: مناقشة نتائج الدراسة

في سبيل الوقوف على مدى اتساق أو اختلاف واقع إدارة المخاطر السيبرانية في البنوك العمومية الجزائرية – محل الدراسة – مع ما أفرزته الأدبيات النظرية والممارسات العالمية ننتقل لمناقشة نتائج الدراسة الميدانية ، و نحو التحليل النقدي وربط النتائج بالفرضيات الأساسية التي انطلقت منها الدراسة، وكذلك مقارنتها بما توصّلت إليه الدراسات السابقة، وفي هذا السياق، سيتمّ مناقشة نتائج كل فرضية على حدة، وربطها بالمؤشرات المستخلصة من الميدان.

أولًا: مناقشة الفرضية الأولى

نص الفرضية" :تواجه البنوك الجزائرية مخاطر سيبرانية متزايدة نتيجة التوسع المستمر في استخدام التكنولوجيات الرقمية والخدمات المصرفية الإلكترونية، مما يزيد من مستوى التهديدات الموجهة إلى نظمها المعلوماتية".

تحليل النتائج: أظهرت نتائج المحور الأول من الدراسة، والمتعلق بمستوى إدراك البنوك العمومية للمخاطر السيبرانية، وجود وعي نسبي لدى مختلف الموظفين المستجوبين بشأن تصاعد حدة هذه التهديدات. فقد أشار أغلبهم (87.5%) إلى أن المخاطر السيبرانية تشكّل تهديدًا حقيقيًا ومتزايدًا، ويرتبط ذلك بشكل مباشر بتوسّع البنوك في تقديم خدمات رقمية عبر الإنترنت، كمنصات المعاملات الإلكترونية والتطبيقات المصرفية.

وبالعودة إلى توزيع آراء الموظفين بين البنوك الثلاثة، لوحظ أن بنك CPA يتمتع بدرجة وعي أعلى نسبيًا نظرًا لحجمه وامتداده المؤسسي مقارنة بـ BEA وBNA، حيث عبّر موظفوه عن قلق أكبر من هجمات مثل الفدية الرقمية أو اختراق قواعد بيانات الزبائن، وهو ما يفسّر التوجه العام نحو المطالبة بتعزيز الأنظمة الأمنية ورفع مستوى التحصين الداخلي.

مقارنة بالدراسات السابقة: تتوافق هذه النتيجة مع ما توصلت إليه دراسة الشلبي (2021)، التي بينت أن البنوك في منطقة المغرب العربي، وعلى رأسها الجزائر، بدأت تدرك أهمية الأمن السيبراني بعد تكرار حوادث الاختراق، دون أن تواكب هذا الإدراك بنية مؤسساتية متكاملة لمجابهة تلك التهديدات.

الاستنتاج: تُؤكد نتائج الدراسة صحة الفرضية الأولى، إذ بيّنت بوضوح أنّ التحول الرقمي المكثف في البنوك الجزائرية لم يكن مصحوبًا بمنظومة حماية موازية تضمن تأمين الأصول الرقمية، مما جعل البنوك عُرضة متزايدة للمخاطر السيبرانية.

ثانيًا: مناقشة الفرضية الثانية

نص الفرضية" :تعتمد البنوك الجزائرية على مجموعة من الوسائل والآليات لإدارة المخاطر السيبرانية، غير أنها لا تزال تعاني من عدة نقائص على مستوى الكفاءات البشرية، والجاهزية التقنية، وكفاءة أنظمة الحماية".

تحليل النتائج: أكدت نتائج المحور الثاني، الذي تناول آليات إدارة المخاطر السيبرانية، أن البنوك تعتمد بالفعل على بعض الآليات مثل جدران الحماية، نظم كشف الاختراق، وتحديثات دورية للبرمجيات، غير أن فعالية هذه الوسائل تُعدّ محدودة. فقد أشار أكثر من 62.5% من المستجوبين إلى وجود فجوات على مستوى التكوين المستمر للموظفين في مجال الأمن السيبراني، إلى جانب ضعف التنسيق بين الوحدات التقنية والإدارية في حالات الطوارئ.

كما نوّه بعض الموظفين إلى غياب نماذج محاكاة للهجمات أو خطط استجابة مرنة، وهو ما يقلّص فعالية تلك الآليات في الواقع العملي. وقد عبّر موظفو BEA على وجه الخصوص عن معاناتهم من تقادم الأنظمة المعلوماتية، مما يزيد من هشاشتها.

مقارنة بالدراسات السابقة: تؤكد هذه النتيجة ما جاء في دراسة بن عيسى وآخرون (2022)، التي اعتبرت أن البنية التحتية التقنية في البنوك الجزائرية متأخرة مقارنة بالمعايير العالمية، وتفتقر إلى التحديثات الدورية الكفيلة برفع مستوى الأمان السيبراني.

الاستنتاج: تُثبِت نتائج المحور الثاني صحة الفرضية الثانية جزئيًا، حيث أن البنوك تمتلك آليات نظرية لإدارة المخاطر، لكنها غير فعالة بالشكل المطلوب، نتيجة لعدة اختلالات على المستوى التقني والبشري والتنظيمي.

ثالثًا: مناقشة الفرضية الثالثة

نص الفرضية: "يشكّل غياب إطار تنظيمي موحد ونقص التكوين المتخصص في الأمن السيبراني أحد أبرز العوائق التي تحدّ من فعالية تطبيق سياسات إدارة المخاطر السيبرانية في البنوك الجزائرية".

تحليل النتائج: أظهر المحور الثالث من الدراسة، والذي تناول العوائق التنظيمية والتكوينية، أنّ غياب التشريع الموحد والسياسات الملزمة على مستوى وطني يُعتبر من أبرز العراقيل، حيث أشار أغلب المستجوبين (75%) إلى أن القوانين الحالية لا تتناول الأمن السيبراني المصرفي بشكل مباشر، بل تكتفي بإشارات عامة ضمن قوانين حماية المعطيات الشخصية أو قانون البريد والاتصالات.

كما تم تسجيل نقص في البرامج التدريبية المتخصصة، وانعدام شراكات مستدامة مع مراكز البحث أو الجامعات في هذا المجال، مما يعمّق من الهوة بين التطور الرقمي ومتطلبات الأمن السيبراني.

مقارنة بالدراسات السابقة: تتقاطع هذه النتيجة مع ما توصلت إليه دراسة سعيداني (2023)، والتي أوضحت أن الإطار التنظيمي للأمن السيبراني في الجزائر لا يزال مشتتًا بين عدة قطاعات، ما ينعكس سلبًا على فعالية الاستجابة الموحدة في القطاع المالي.

الاستنتاج: تدعم النتائج الميدانية صحة الفرضية الثالثة بشكل قوي، وتدلّ على ضرورة تدخل الجهات التنظيمية الوطنية، مثل بنك الجزائر ووزارة المالية، لإصدار تشريعات ملزمة ومتكاملة تعالج الأمن السيبراني كأولوية استراتيجية.

رابعًا: مناقشة الفرضية الرابعة

نص الفرضية: "يُعتبر التكامل بين التحول الرقمي واستراتيجية الأمن السيبراني عنصرًا حاسمًا في تعزيز قدرة البنوك الجزائرية على مواجهة المخاطر السيبرانية، وذلك انطلاقًا مما تكشف عنه المعطيات الميدانية وآراء الفاعلين في القطاع البنكي".

تحليل النتائج: بيّن المحور الرابع من الدراسة إدراكًا متزايدًا لدى الفاعلين في البنوك العمومية بأهمية التكامل بين الرقمنة والأمن، إذ عبّر 87.5% من المستجوبين عن ضرورة تضمين الأمن السيبراني في كل مرحلة من مراحل الرقمنة، بدءًا من تصميم الخدمات الرقمية، مرورًا بتطوير التطبيقات، وصولًا إلى مراحل التشغيل والصيانة.

لكن الميدان يعكس وجود فجوة بين هذا الوعي النظري والتطبيق العملي، إذ لا توجد حاليًا استراتيجية رقمية مدمجة تتضمن الأمن السيبراني كركيزة أساسية، وإنما يتم التعامل مع الجانبين بشكل منفصل، مما يؤدي إلى ضُعف في الاستجابة الفعالة للمخاطر.

مقارنة بالدراسات السابقة: تتطابق هذه النتيجة مع ما خلصت إليه دراسة KPMG (2022) حول البنوك في شمال إفريقيا، والتي أوصت بإدماج الأمن السيبراني منذ مرحلة التخطيط الرقمي، عبر ما يعرف بـ"الأمن حسب التصميم(Security by Design) "، لضمان المرونة والتكامل.

الاستنتاج: النتائج تدعم الفرضية الرابعة، وتؤكد أن فعالية التصدي للمخاطر السيبرانية تتوقف على مدى تكامل استراتيجية التحول الرقمي مع سياسات الأمن، وأن غياب هذا التكامل يجعل النظام المالي أكثر عرضة للتهديدات، رغم التقدم النسبي في البنية التحتية الرقمية.

وفي ضوء ما سبق تحليله ومناقشته من نتائج ميدانية وفرضيات بحثية، يتضح أن تعامل البنوك العمومية الجزائرية مع المخاطر السيبرانية في ظل التحول الرقمي لا يزال في طور التأسيس والتطور، إذ أن هذا التعامل يتسم بطابع جزئي ومحدود، تغلب عليه المقاربة الدفاعية الظرفية أكثر من كونه توجهًا استراتيجيًا طويل المدى. فرغم وجود وعي متزايد لدى الفاعلين البنكيين بخطورة هذه التهديدات الرقمية، خاصة في ظل التوسع الملحوظ في استخدام الخدمات المصرفية الإلكترونية، إلا أنّ البنوك المعنية لم تبلور بعد منظومة أمنية شاملة ومتكاملة لإدارة هذه المخاطر ضمن إطار مؤسساتي وقانوني موحد.

وقد أظهرت النتائج الميدانية أن هذه المؤسسات تعتمد حاليًا على وسائل تقنية مشتتة، غالبًا ما تكون غير محدثة أو غير مدعّمة بكفاءات بشرية مؤهلة، إلى جانب افتقارها لاستراتيجيات داخلية واضحة في مجال الأمن السيبراني. كما تعاني من هشاشة التنسيق بين التحول الرقمي والتأمين السيبراني، الأمر الذي يزيد من درجة التعرّض للاختراقات والتهديدات الإلكترونية.

وبالتالي، فإنّ الإجابة عن إشكالية الدراسة تقودنا إلى التأكيد بأن تعامل البنوك الجزائرية مع المخاطر السيبرانية في ظل التحول الرقمي يتميّز حاليًا بعدة اختلالات هيكلية، تتطلب إعادة نظر شاملة في المنظومة السيبرانية، سواء على مستوى التشريع الوطني، أو على مستوى سياسات التكوين، أو من خلال الاستثمار في تقنيات حديثة تواكب التحولات الرقمية المتسارعة، وتتماهى مع معايير الأمن المصرفي المعتمدة دوليًا.

خلاصة الفصل :

من خلال هذا الفصل، تم التطرق إلى عرض وتحليل ومناقشة نتائج الدراسة الميدانية، التي أُجريت على عينة مكوّنة من ثمانية موظفين موزعين على ثلاثة فروع للبنوك العمومية بورقلة CPA ، BEA، BNA وقد تمّ تنظيم النتائج حسب أربعة محاور رئيسية، كل منها مرتبط بإحدى الفرضيات الأساسية للدراسة.

أظهرت النتائج أن البنوك الجزائرية تواجه مخاطر سيبرانية فعلية ومتزايدة، تتجلى في تعدد أنواع التهديدات وتكرار محاولات الاختراق، وهو ما أكده أغلب المستجوبين. كما بيّنت الدراسة أن الوسائل الحالية المعتمدة لمواجهة هذه التهديدات، سواء كانت تقنية أو تنظيمية، تبقى غير كافية في ظل النقص الواضح في التكوين المتخصص، وضعف التنسيق بين الإدارات، وغياب رؤية استراتيجية موحدة.

كذلك تم رصد عوائق مؤسساتية وهيكلية تحدّ من فعالية إدارة الأمن السيبراني، أبرزها غياب الإطار التنظيمي الموحد، وقلة الوعي في بعض المستويات بأهمية الأمن السيبراني، إلى جانب التكوين غير المنتظم للموظفين. أما فيما يخص العلاقة بين التحول الرقمي والأمن السيبراني، فقد تبيّن أن هذا التكامل لا يزال ضعيفًا، وغالبًا ما يُنظر إلى كل مجال بمعزل عن الآخر داخل البنوك محل الدراسة.

وفي الأخير، ومن خلال تحليل الفرضيات ومناقشة النتائج، يمكن القول إن إدارة المخاطر السيبرانية في البنوك الجزائرية تمر بمرحلة انتقالية حرجة، تتطلب جهودًا متعددة المستويات: على صعيد التكوين، والتشريع، والتحديث التكنولوجي، وذلك لضمان تحول رقمي آمن وفعّال.

الخاتمة

خاتمة

يُعد الأمن السيبراني اليوم من بين أبرز الرهانات الإستراتيجية التي تواجه النظم المصرفية في ظل التوسع المطرد في استخدام التكنولوجيا المالية والتحول الرقمي الشامل. وإذا كانت الرقمنة قد أصبحت خيارًا وجوديًا للمؤسسات المالية، فإنها في الوقت ذاته فتحت الباب واسعًا أمام تهديدات غير تقليدية، تتجاوز البنية المادية للمؤسسة إلى صميم أمنها المعلوماتي واستقرارها المؤسسي. وانطلاقًا من هذا الواقع، جاءت هذه الدراسة لتسلط الضوء على الوضعية الواقعية للأمن السيبراني داخل البنوك العمومية في الجزائر، وتحديدًا على مستوى ولاية ورقلة، في سياق التحول الرقمي.

أظهرت النتائج المستخلصة من التحليل الميداني أن البنوك العمومية المعنية بالدراسة تدرك، بدرجات متفاوتة، أهمية الأمن السيبراني وضرورة إدماجه في سياسات التحول الرقمي، إلا أن هذا الإدراك لم يُترجم بعد إلى استراتيجيات مؤسساتية ملموسة ومتكاملة. فما يزال التعامل مع المخاطر السيبرانية يتم بصفة مجزأة، وفي إطار ردّ الفعل بدل الاستباق، ما يعكس غياب ثقافة مؤسسية متجذرة في هذا المجال. كما أن الهياكل التقنية المتوفرة تُعاني من هشاشة على مستوى التجهيزات، ومن ضعف في الكفاءات المتخصصة، ناهيك عن محدودية التنسيق بين الإدارات الداخلية، وغياب مرجعية معيارية موحدة للتعامل مع الهجمات السيبرانية.

من جهة أخرى، فإن نتائج الدراسة أثبتت وجود وعي أولي لدى الموظفين بأهمية الأمن السيبراني، إلا أن هذا الوعي يصطدم بجملة من التحديات الميدانية، أبرزها: غياب التكوين المتخصص والدوري، وعدم ملاءمة برامج الحماية المستخدمة مع خصوصية التهديدات الرقمية المتزايدة، إلى جانب نقص الموارد المالية الموجهة لتدعيم الحماية المعلوماتية. كما أبانت النتائج عن غياب بنية تنظيمية واضحة تُعنى حصريًا بالأمن السيبراني في هيكل البنك، ما يُضعف من فعالية الاستجابة للطوارئ ويحد من قدرة المؤسسات على تطوير بروتوكولات أمنية داخلية.

مقترحات الدراسة

استنادًا إلى المعطيات السابقة، فإن هذه الدراسة تقترح مجموعة من التدابير العملية الآتية:

- إعادة هيكلة نظم الحوكمة الرقمية داخل البنوك العمومية، من خلال استحداث وحدات خاصة بالأمن السيبراني تُدار بكفاءات مختصة وتكون على اتصال مباشر بالإدارة العليا.
- بلورة خارطة طريق وطنية للأمن السيبراني المصرفي، تتضمن أطرًا تنظيمية وتشغيلية موحّدة لمجابهة التهديدات الرقمية المتصاعدة.

- تحفيز الاستثمارات التكنولوجية الذكية، خاصة تلك التي تعتمد على الذكاء الاصطناعي والتحليل التنبؤي في رصد وتحييد المخاطر السيبرانية.
- إدراج الأمن السيبراني في برامج التكوين الأولي والمستمر، بما يضمن بناء رأس مال بشري قادر على التعامل مع المستجدات الرقمية بأعلى درجات الاحترافية.

التوصيات

- ضرورة إصدار تشريع خاص بالأمن السيبراني المصرفي، يُلزم البنوك بوضع خطط استجابة للطوارئ، وتحيين أنظمتها الأمنية بصفة دورية.
- إدراج مؤشرات الأمن السيبراني ضمن أدوات التقييم السنوي لأداء المؤسسات البنكية.
- تنصيب هيئة إشراف وطنية تُعنى بمتابعة وتنظيم الأمن السيبراني في القطاع المالي والمصرفي.
- خلق شراكات مع الجامعات ومراكز البحث بهدف تطوير حلول محلية متقدمة في مجال الأمن السيبراني.

آفاق البحث المستقبلية

بما أن موضوع الأمن السيبراني في المؤسسات البنكية لا يزال حديث النشأة نسبيًا في البيئة الجزائرية، فإن هذه الدراسة تمهد الطريق لعدة أبحاث مستقبلية ممكنة، من أبرزها:

- دراسة تأثير الكفاءات البشرية المتخصصة في تكنولوجيا المعلومات على فعالية الأمن السيبراني البنكي.
- تحليل تجربة بنك الجزائر المركزي في حماية البنية التحتية الرقمية وتعميمها على البنوك التجارية.
- دراسة مدى ملاءمة الأطر القانونية الوطنية لمتطلبات الحماية السيبرانية في البيئة المالية.
- مقارنة بين مستوى الأمن السيبراني في البنوك الجزائرية والمؤسسات البنكية في دول مغاربية أو نامية مماثلة.

وبناءً على ما تقدّم، تُبيّن الدراسة أن التحول الرقمي داخل البنوك لا يمكن أن يُكتب له النجاح بمعزل عن رؤية شمولية للأمن السيبراني، قوامها الحوكمة الفعّالة، والتكوين المستمر، والاستثمار الذكي في التكنولوجيا. فالرهان اليوم لم يعُد فقط على سرعة التحول، بل على مدى متانته ومقاومته للتهديدات، لأن النظام المالي الحديث لا يتهاوى غالبًا من الخارج، بل من ثغرة رقمية صغيرة لم تُؤخذ بالجدية الكافية.

قائمة المراجع والمصادر

قائمة المراجع والمصادر

أولاً ; الكتب والمراجع العلمية

- العمري، عبد الحكيم. الرقمنة والتحول في المؤسسات المصرفية العربية. عمان: دار صفاء للنشر، 2020.

ثانياً: المذكرات العلمية

- بن صالح، محمد. تحليل واقع المخاطر السيبرانية في البنوك العمومية الجزائرية. مذكرة ماجستير، جامعة قاصدي مرباح ورقلة، 2021.
- بن عيسى، سميرة. التحول الرقمي في البنوك الجزائرية كآلية لتحسين جودة الخدمة المصرفية. مذكرة ماجستير، جامعة البليدة 2، 2020.
- بن قادة، سارة، وبوجلال، سهام. فاعلية استراتيجيات الأمن السيبراني في البنوك الجزائرية. مذكرة ماجستير، جامعة الجزائر 3، 2021.
- بن كينة، حياة. دور التحول الرقمي في تحسين الأداء المالي في البنوك – دراسة حالة القرض الشعبي الجزائري. مذكرة ماجستير، جامعة غرداية، 2024.
- بن نعمية، ملاك، بن بوزيد، إيمان، ودبابسة، نعيمة. التحول الرقمي الذكي في بنك الفلاحة والتنمية الريفية – دراسة حالة وكالة الوادي. مذكرة تخرج، جامعة الوادي، 2023.
- بوعلي، مروى. التحول الرقمي كخيار استراتيجي للبنوك الجزائرية: دراسة حالة بنك التنمية المحلية. مذكرة ماجستير، جامعة قاصدي مرباح ورقلة، 2022.
- بوزادية، جمال. فاعلية استراتيجيات الأمن السيبراني في البنوك الجزائرية. مذكرة ماجستير، كلية العلوم الاقتصادية، جامعة الجزائر 3، 2021.
- بوشيخي، مونية. دور الرقمنة في تعميم الشمول المالي بالجزائر. مذكرة ماجستير، جامعة الجزائر 3، 2022.
- بركاني، سهيلة. فاعلية استراتيجيات الأمن السيبراني في البنوك الجزائرية – دراسة حالة بنك التنمية المحلية. مذكرة ماجستير، جامعة الجزائر 3، 2021.
- دقيش، حفيظة. دور الرقمنة في تحسين جودة الخدمات البنكية. مذكرة ماجستير، جامعة الجزائر 3، 2021.
- راهب، سناء، وشابي، حليمة. أثر التحول الرقمي على الأداء الوظيفي في البنوك التجارية الجزائرية. مذكرة ماجستير، جامعة الطارف، 2023.

- سعدية، مداني، وصباح، طويري. تحليل واقع التحول الرقمي في البنوك العمومية الجزائرية. مذكرة ماجستير، جامعة قاصدي مرباح ورقلة، 2021.
- عشي، سفيان. أثر التحول الرقمي على أداء البنوك التجارية الجزائرية. مذكرة ماجستير، جامعة الجزائر 1، 2022.
- عيساوي، ياسين. دور الرقمنة في تعميم الشمول المالي في الجزائر – دراسة حالة بنك السلام. مذكرة ماجستير، المركز الجامعي بالنعامة، 2022.
- لخضاري، سامية. تحليل واقع الأمن السيبراني في البنوك الجزائرية. مذكرة ماجستير، جامعة قسنطينة 2، 2021.
- زروقي، عبد الحفيظ. تحليل واقع المخاطر السيبرانية في البنوك العمومية الجزائرية – دراسة ميدانية ببنك BADR. مذكرة ماجستير، جامعة قاصدي مرباح ورقلة، 2021.

ثالثاً: المقالات العلمية

- بن زيد، عبد القادر. "إدارة المخاطر السيبرانية في المؤسسات المالية: دراسة تحليلية". مجلة العلوم الاقتصادية، جامعة الجزائر، 2020.
- جودي، محمد. "محددات تبني الرقمنة في البنوك الجزائرية". مجلة الاقتصاد الجديد، العدد 18، 2022.
- غربي، علي. "التحول الرقمي في المؤسسات الجزائرية: الواقع والتحديات". مجلة أبحاث اقتصادية، العدد 11، 2021.

رابعا : التقارير الرسمية والمنشورات الحكومية

- اللجنة الجزائرية للرقابة المصرفية .(COSOB) نشرة تنظيمية حول التحديات الرقمية للبنوك، العدد 03، الجزائر، 2022.
- المديرية العامة لأمن نظم المعلومات. تقرير داخلي غير منشور. وزارة الرقمنة والإحصائيات، الجزائر، 2023.
- منظمة التعاون الاقتصادي والتنمية (OECD). تقرير الأمن السيبراني للنظام المالي. باريس، 2019.

خامسا : الدراسات الأجنبية

- Baskerville, Richard. Cybersecurity Risk Management: A Review of Approaches and Challenges. Information Systems Management, 2018.
- Bloxham, Peter. Digital Transformation in Financial Services: The Role of Cyber Risk Management. The London Institute of Banking & Finance, 2020.
- Gordon, L. A., & Loeb, M. P. "The Economics of Information Security Investment." ACM Transactions on Information and System Security, Vol. 5, No. 4, 2002.
- Lagarde, Christine. The Financial Sector Must Take Cyber Risk More Seriously. World Economic Forum, 2017.
- https://www.weforum.org/agenda/2017/01/financial-sector-cyber-risk
- OECD. Cybersecurity Risk Management for Financial Stability, 2021.
- https://www.oecd.org/finance/Cybersecurity-Risk-Management.pdf
- OECD. Digital Transformation in Financial Services, 2021.
- https://www.oecd.org/digital/digital-transformation-in-financial-services.pdf
- Opderbeck, David W., & Kerr, Orin S. "The Law of Cybersecurity and the Financial Sector." The Journal of Financial Regulation, 2021.
- Pfleeger, C. P., & Pfleeger, S. L. Security in Computing, 5th ed. Pearson Education, 2012.
- Schneier, Bruce. Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. Norton & Company, 2015.
- Interbank. Digital Transformation in Financial Sector, 2021.