

حوكمة البنوك العمومية الجزائرية كألية لإدارة مخاطر الامن السيبراني في ظل استخدامات الذكاء الاصطناعي -دراسة حالة عينة من البنوك العمومية الجزائرية-

Governance of Algerian public banks as a mechanism for managing cybersecurity risks in the context of artificial intelligence: a case study of a sample of Algerian public banks

مباركة دلامي¹، محمد يونس²

¹ ط.د، المركز الجامعي تيبازة، Delami.mebarka@cu-tipaza.dz

² بروفيسور التعليم العالي، المركز الجامعي تيبازة، m.younsi@mesrs.dz

مخبر الاقتصاد و التنمية

الاستلام: 02-07-2025 القبول: 01-10-2025

ملخص:

مع تنامي استخدام الذكاء الاصطناعي في تحسين كفاءة القطاع المصرفي كاستجابة لمخرجات الثورة الرقمية العالمية، وجدت البنوك نفسها وسط تقنيات جديدة ومتطلبات رقمية محفوفة بالمخاطر السيبرانية وهو ما اجبر الهيئات الدولية والرقابية وكذا الاشرافية الى تبني حوكمة الامن السيبراني لمحاربة المخاطر السيبرانية التي باتت تهدد نشاط البنوك الرقمي.

تبنّت البنوك العمومية الجزائرية حوكمة الامن السيبراني وتأمين قواعد البيانات والبنى الرقمية ضمن أولوياتها، وهو ما يعكس النتائج الإيجابية المتوصل اليها، متمثلة في نجاح البنوك في تفادي المخاطر السيبرانية وتقزيم الخسائر المتعلقة بها.

كلمات مفتاحية: الذكاء الاصطناعي، الثورة الرقمية، حوكمة الامن السيبراني، المخاطر السيبرانية.

Abstract:

With the growing use of artificial intelligence in improving the efficiency of the banking sector as a response to the outputs of the global digital revolution, banks found themselves in the midst of new technologies and digital requirements fraught with cyber risks, which forced

international regulatory and supervisory bodies to adopt cybersecurity governance to combat cyber risks that threaten the digital activity of banks.

Algerian public banks have prioritised cybersecurity governance and securing databases and digital infrastructures, which reflects the positive results achieved, represented by the success of banks in avoiding cyber risks and minimising losses related to them.

Keywords: Artificial Intelligence; Digital Revolution; Cybersecurity Governance; Cyber Risks.

المؤلف المراسل: مباركة دلامي، الإيميل: Delami.mebarka@cu-tipaza.dz

1. مقدمة :

استجابة للتكنولوجيا الرقمية و استخدامات الذكاء الاصطناعي، قامت البنوك بإدخال ابتكارات مصرفية جديدة و خدمات رقمية حديثة و متطورة، و كوجه اخر لهاذ التطورات ظهرت مخاطر جديدة منها مخاطر الامن السيبراني، و اصبحت تحديد حقيقي للبنك يعوق من استمراريته في حفظ امان عملائه، و هذا ما دفع بصناع القرار في القطاع المالي و المصرفي الى تعزيز حوكمة القطاع ضد الهجمات السيبرانية. بالرغم من حداثة عهد البنوك الجزائرية بالتكنولوجيا الرقمية، إلا أن القطاع المصرفي في الجزائر يسعى لمواكبة التحولات العالمية، و هو ما دفع بالبنوك الجزائرية الى دمج التكنولوجيا ضمن خدماتها المصرفية وهذا ما يدفعنا لطرح التساؤل التالي:

ما مدى جاهزية الحوكمة البنكية والبنى التحتية التقنية للأمن السيبراني في البنوك العمومية

الجزائرية لمواجهة مخاطر الامن السيبراني؟

للإجابة على الإشكالية، ارتأينا طرح الفرضيات الآتية:

- تُساهم الحوكمة في تعزيز حماية البنوك العمومية الجزائرية من الهجمات السيبرانية؛
- حوكمة الامن السيبراني في البنوك العمومية الجزائرية يقلل من حجم الخسائر السيبرانية؛
- يساهم التزام الإدارة العليا في البنوك العمومية الجزائرية بمبادئ حوكمة الأمن السيبراني في تحسين مستوى الأمن السيبراني.

اهداف الدراسة

- تحليل مدى تطبيق حوكمة الأمن السيبراني في البنوك العمومية الجزائرية وقياس دورها في التقليل من الخسائر الناتجة عن المخاطر السيبرانية؛
- تشخيص أهم التهديدات والمخاطر السيبرانية التي تواجه نشاط البنوك في الجزائر؛
- تقييم مدى التزام البنوك العمومية الجزائرية بالإرشادات والمعايير الدولية ذات الصلة.

منهجية البحث

تم الاعتماد على المنهج الوصفي لتحليل المفاهيم النظرية المتعلقة بحوكمة الأمن السيبراني والمخاطر السيبرانية، كما تم الاستعانة بالمنهج التحليلي لدراسة الواقع التطبيقي داخل البنوك العمومية الجزائرية في المجال.

2. حوكمة البنوك في ظل استخدامات الذكاء الاصطناعي

1.2 حوكمة البنوك:

1.1.2 مفهوم حوكمة البنوك: تعنى الحوكمة بإدارة البنك والعلاقات بين ذوي المصالح من مجلس ادارة الى مساهمين الى عملاء والحد من أخطار تضارب المصالح، وتسعى الحوكمة الى تبيان العلاقة بين كل الاطراف ذات الصلة وتحديد المسؤوليات والصلاحيات و السهر على مراقبة الاداء وتحقيق اهداف البنك و حماية حقوق العملاء و ادارة المخاطر المحيطة بعمل البنك و المخاطر المحتملة مع رسم استراتيجية واضحة المعالم لقيادة المنشأة (**Jean & Viviane** , 2016).

2.1.2 أهداف حوكمة البنوك (محسن الربيعي و عبد الحسين راضي، 2020، الصفحات 12-13):

- وضع استراتيجية كفيلة بتحقيق أكبر العوائد ؛
- ضبط العلاقات بين مجلس الادارة و مختلف اصحاب المصالح؛

- تطوير نظام رقابة و اشراف على اداء البنك و مدى التزامه بالقوانين و اللوائح؛
- الرقابة على النشاط و التحكم في المخاطر و ادارتها و انتهاج اساليب التحوط منها؛
- خلق بيئة و نظام تحفيزي للعمال.

3.1.2 مبادئ حوكمة البنوك وفق لجنة بازل للرقابة المصرفية (اللجنة العربية للرقابة المصرفية،

2017، الصفحات 8-38): سعت لجنة بازل الى تحديث هذه المبادئ وفق المتغيرات

الاقتصادية، حيث نشرت في اخر ورقة محدثة لها المبادئ التالية:

- كفاءة اعضاء مجلس الإدارة و استقلاله: منحه استقلالية اكبر مع تسليط الضوء على مؤهلات اعضاء مجلس الادارة، حيث نصت على ضرورة توفير تركيبة مؤهلة و كفؤة من اجل تنفيذ استراتيجية البنك و تحقيق اهدافه؛
- سياسة ادارة المخاطر: توفير وظيفة ادارة المخاطر في كل بنك و يجب ان يكون الموظفون ذوو كفاءة عالية و خبرة و مؤهلات تسمح لهم بتحديد و رصد المخاطر و ضبطها؛
- الامتثال و التدقيق الداخلي: الامتثال للقوانين و اللوائح التنظيمية في القطاع المصرفي امر ضروري و يقع على عاتق مجلس الادارة، كما تسعى اللجنة الى تعزيز دور المراجعة الداخلية بالبنك؛
- الافصاح و الشفافية: البنك ملزم بالإفصاح و الشفافية عن كل الانشطة امام المساهمين و كل اصحاب المصالح و ذلك بتقديم تقارير صحيحة و دقيقة حول الوضع المالي للبنك و السياسة المتبعة و المخاطر المحتملة ، و الاستراتيجيات المستقبلية؛
- دور السلطات الإشرافية: من خلال مراقبة الامتثال و التدخل عند الضرورة إضافة الى التواصل المستمر مع كل البنوك.

2.2 أوجه استخدامات الذكاء الاصطناعي AI في القطاع المصرفي:

- ترتيب الجدارة الائتمانية للعملاء و تسهيل عملية الاقراض (بن خضرة و بضيف، 2024، صفحة 282)؛

• روبوتات الدردشة: انتشرت هذه الظاهرة بعد انتشار وباء كورونا، حيث فضل العملاء التعاملات المالية الرقمية عن بعد و هذا ما اتاحه لهم روبوتات الدردشة (shambhavi, 2022)؛

• تعزيز الامن السيبراني المصرفي و مكافحة المخاطر: يساهم الذكاء الاصطناعي في تعزيز امان و كفاءة العمليات المصرفية خصوصا الرقمية منها، و ذلك من خلال تحليل سلوك العملاء و اكتشاف الثغرات الامنية عن طريق رصد السلوكيات غير النمطية في معاملاتهم، كما يستخدم في التنبؤ بالمخاطر مثل غسيل او تهريب الاموال و التحويلات المشبوهة (رجب عبد العظيم، 2024).

الجدول 01: مجالات استخدام الذكاء الاصطناعي في الصناعة المصرفية في العالم لسنة 2020

النسبة المئوية لاستخدام الذكاء الاصطناعي %	مجالات الخدمات المالية	
58	كشف الاحتيال	1
41	تحليل العمليات المالية	2
33	الامن السيبراني	3
33	تخصيص المنتجات و الخدمات	4
31	رعاية العملاء	5
25	صيانة الاصول	6

المصدر: علي بن الضب، 2023، ص27.

تحتل تطبيقات كشف الاحتيال الصدارة بنسبة 58 % ، اما استخدام ال AI في تحليل العمليات المالية بلغ نسبة 41% نظرا لقدرته على استيعاب البيانات الضخمة و تحليلها، اما استعماله في الامن السيبراني فقد بلغ نسبة 33 % و هو ما يعكس سعي الدول و الانظمة الى حماية بيانات العملاء و الحد من التهديدات الالكترونية المتزايدة ، في حين بلغت نسبة استخدامه في تخصيص المنتجات و

الخدمات نسبة 33 %، اما رعاية العملاء و صيانة الاصول المالية بلغتا على التوالي 31 % و 25 % اذ تعتبر روبوتات الدردشة الذكية قفزة نوعية في خدمة العملاء و صيانة و حماية الاصول المالية عن طريق التنبؤ المسبق من خلال تحليل البيانات التاريخية و ادارة المخاطر التشغيلية.

3. الامن السيبراني في البنوك

1.3 الامن السيبراني كتوجه حتمي:

قدر البنك الدولي نسبة 65 % كمخاطر الهجمات الالكترونية التي تواجه القطاع المصرفي (اسماعيل احمد البردوني، 2025، صفحة 11)، و هي نسبة تعتبر مرتفعة نظرا لحساسية القطاع و اهميته و هو ما دفع بالجهات التنظيمية و الاشرافية الى تعزيز حوكمة الامن السيبراني كتوجه حتمي تقتضيه مخلفات الثورة الرقمية و التكنولوجيا بالقطاع:

1.1.3 مفهوم الامن السيبراني: لا يوجد تعريف موحد بل هناك عدة تعريفات حسب اختصاص

و اهداف كل جهة، نذكر منها:

- تعريف المنظمة الدولية للمعايير **ISO**: "البرنامج الذي من خلاله يمكن ضمان سرية و سلامة الانظمة و البرمجيات و توافر المعلومات في الفضاء السيبراني" (**ISO/IEC 27032:2023**, 2023) ؛

- تعريف قاموس اكسفورد: الاجراءات المتخذة من اجل تحقيق الحماية من الاستخدام الاجرامي او غير المصرح به للبيانات الالكترونية (زمورة و بن عيسى ، 2022، صفحة 416) .

من خلال كل ما سبق ، يمكن تعريف الامن السيبراني على انه علم مستمر و يواكب كل التحديات و التطورات التكنولوجية يجمع بين مختلف البرمجيات و السياسات و الضوابط و كذا المبادئ ناهيك عن الانظمة التي من شأنها حماية الفضاء السيبراني (معلومات، شبكات و انظمة رقمية) من التلف او/و من كل اختراق او تجسس او ابتزاز او وصول غير مصرح.

2.1.3 نجاعة الامن السيبراني في حماية البيانات و الانظمة:

- الحفاظ على السرية: يعزز الامن السيبراني سرية البيانات و المعلومات الشخصية و يحول دون الوصول غير المرخص لها او الاستخدام غير القانوني لها، كما يضمن سلامتها و توافرها في الوقت المحدد (طواهير، 2023، صفحة 282)؛
- الوصول الى بنية معلوماتية تقنية متينة: بناء نظام تقني و وضع خطط استباقية تجهيزية لمواجهة المخاطر اضافة الى نشر الوعي و الثقافة الامنية (سعيد قاسم القدسي، 2024، صفحة 370)؛
- اثبات الجريمة السيبرانية: يقطع الامن السيبراني اشواطاً مهمة في اثبات الجريمة السيبرانية و معاقبة المجرمين (سي عبد القادر، 2024، الصفحات 24-28).

2.3 المخاطر السيبرانية في البنوك:

وفقاً للشركة المتخصصة في الامن السيبراني Guidewire فان نسبة تعرض احد البنوك في القطاع المصرفي الى هجوم سيبراني تبلغ 34.3 % (P Global Ratings&S، 2024)، اذ تقدر خسائر الهجمات السيبرانية ب 2.5 مليار دولار على الاقل (صندوق النقد الدولي، 2024)، و هو ما يحتم على الجهات الرقابية و الاشرافية تعزيز ممارسات الامن السيبراني في القطاع المصرفي:

1.2.3 المخاطر السيبرانية التي تعترض النظم المصرفية:

- القرصنة و الاختراق: يتم اختراق النظم و البرامج الالكترونية و الوصول اليها و تدمير البنية التحتية المعلوماتية المالية (حارس محمد طه ابو الخير، 2023، صفحة 24)؛
- البرمجيات الخبيثة: زرع البرمجيات الخبيثة في انظمة الحواسيب عن طريق الرسائل الالكترونية التصيدية (فتحي السيد البغدادي، 2021، صفحة 1476)؛

- **انتحال الموقع:** انتحال موقع البنك على الانترنت بموقع ويب مشابه تماما، حيث يتم سرقة بيانات المستخدمين عند دخولهم الموقع المزيف (جغل و زفرير، 2023، صفحة 308)؛
- **هجمات XSS:** استغلال صفحات الويب التي يلج اليها المستخدمين و تحويلهم الى مواقع ضارة موازية. (رجب عبد العظيم، 2024)

2.2.3 تحديات الامن السيبراني في البنوك:

- **البنية التحتية التقنية:** تطوير الانظمة و البرمجيات و تعزيز الخوادم التي تحفظ الاصول التقنية و بيانات العملاء وتطوير منصات التبادل الرقمي (حارس محمد طه ابو الخير، 2023، صفحة 24)؛
- **الموازنة بين درجة الامان و راحة المستخدم:** الحرس على الموازنة بين الامان و راحة المستخدم لتوفير مرونة الكترونية تتناسب و رغبات العملاء (Léa, 2023) ؛
- **الكفاءة المتطورة:** توظيف كفاءات ذات مهارات عالية و خبراء في المجال السيبراني، كما يتم الاستعانة بمصادر خارجية متخصصة في مجال الامن السيبراني (مزودي الخدمات الخارجيين) (cyber management school, 2024)؛
- **تحديات القوانين و التشريعات:** يجب توفير فضاء آمن لممارسة العمليات المصرفية الرقمية المختلفة، ومكافحة الجريمة السيبرانية و معاقبة المتسببين في اي هجوم او ضرر (علي خميس ابراهيم كعموش، 2024، صفحة 915)؛

4. الجهود الجزائرية في حوكمة الامن السيبراني بالبنوك العمومية الجزائرية:

1.4 الارادة الجزائرية لرقمنة القطاع المالي و المصرفي:

1.1.4 تطور الدفع الالكتروني: إطلاق نظام الدفع الالكتروني في أكتوبر 2016 لحاملي البطاقات

البنكية CIB او البطاقة الذهبية لبريد الجزائر، مدعوما بأنظمة الصيرفة الالكترونية:

- شركة **SATIM**: تعمل على تطوير طرق الدفع الالكتروني، ادارة المنصة التقنية للصيرفة

الالكترونية و تدعم البنوك في تطوير التقنيات الالكترونية (بن شلاط، 2022، صفحة 103)؛

- النظام الجزائري **RTGS** للتسوية الاجمالية الفورية **Real Time Gross settlements**:

نظام التسوية بين البنوك للمبالغ الكبيرة، يهدف الى تحديث النظام المصرفي وفق المقاييس الدولية في

مجال المخاطر، كما تتم به تسوية مبالغ المقاصة الالكترونية (كراع، العمل المصرفي الالكتروني و

المسؤولية المدنية للبنك فيه، 2021، صفحة 15)؛

- نظام **Algérie ATCI**

Interbancaire Compensation Télé المكمل لنظام **RTGS** : نظام للمقاصة عن

بعد، يرمي الى مرافقة عصنة نظام الدفع و رقمته و مواكبته للمعايير الدولية، و تقليص آجال المعالجة

(banque d'lagerie, 2005)؛

2.1.4 أحدث التشريعات التي ترافق الجزائر في مشروع الرقمنة:

- القانون **09-23**: قامت الجزائر بتحيين و عصنة القانون النقدي و المصرفي لدعم مسار الرقمنة و

ذلك من خلال:

استحداث لجنة الاستقرار المالي: مكلفة بالرقابة الاحترازية الكلية و الادارة الفعالة للالزمات و

المخاطر بما فيها تلك المنجرة عن التحول الرقمي ؛

اللجنة الوطنية للدفع: مكلفة بتطوير مشروع تطوير وسائل الدفع الالكترونية من اجل ارساء

الشمول المالي؛

الدينار الرقمي الجزائري: توسيع وسائل الدفع لتشمل الشكل الالكتروني (رنان، 2023،

صفحة 292).

- النظام 04-24 المؤرخ في 13 أكتوبر 2024: يتعلق بالشروط الخاصة للترخيص بتأسيس و

اعتماد ممارسة نشاط البنك الرقمي ، حيث نص على (بنك الجزائر، 2024):

المادة 2: "البنك الرقمي هو كل بنك يقدم خدمات و منتجات مصرفية حصريا عبر

الدعائم او المنصات الرقمية"؛

المادة 6: "يجب ان يؤسس البنك مقرا اجتماعيا لتلقي الشكاوي و من اجل الاغراض

الادارية".

3.1.4 متطلبات نجاح الامن السيبراني ورقمنة الخدمات المصرفية في الجزائر:

• البنية التحتية التقنية: شهدت البنوك الجزائرية مؤخرا جملة من التطورات:

- دمج التكنولوجيا الرقمية والخدمات الالكترونية في نشاطها؛

- ظهور الصيرفة الهاتفية وادخال التطبيقات الرقمية و روبوتات الدردشة التي تسمح للعملاء بإدارة

حساباتهم عن بعد؛

- استحداث الوكالات الرقمية الالكترونية (فنيش و نجار، 2024، الصفحات 158-161).
 - الكوادر التقنية: حرص المشرع الجزائري على منح رخصة فتح البنوك الى مؤسسين اكفاء و ذوو سجل تاريخي نظيف بعيدا عن الشبهة و كذا شروط توافر الخبرة و مهارات قيادية و معرفية فعالة في المجال المصرفي بموجب المادة 3 من النظام 01-24 و المادة 6 من النظام 05-92؛ (كرام و ناوي، 11 ديسمبر 2024)؛
 - البيئة التشريعية: و هو ما نصت عليه وثيقة لجنة بازل في النقطة 5.30 اهمية البنية التحتية العامة المتطورة ، على ضرورة توافر بيئة محاسبية و تدقيقية واضحة المعالم تتمتع بقبول دولي و وضع معايير اخلاقية شفافة و معايير تقنية الزامية على المسيرين و المهنيين (Basel Committee on Banking Supervision, 2023, p. 20) ؛
- 2.4 حوكمة الامن السيبراني في البنوك العمومية الجزائرية:
- 1.2.4 تشريعات الامن السيبراني في الجزائر:
- قانون الوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال: رقم 09-04 المؤرخ في 05 اوت سنة 2009 ، الذي عرف فيه الجريمة السيبرانية و اشار فيه الى الجرائم التي تمس انظمة المعلومات (بارة، 2017، صفحة 266)؛
 - القانون 04-15 الجرائم المتصلة بالمعالجة الآلية للمعطيات (بن علي، 2022، صفحة 314):
نص على معاقبة كل من:

- الدخول غير المصرح: اي اختراق او دخول غير مصرح به الى النظام المعلوماتي للغير، ينجر عنه متابعة قضائية؛

- التزوير المعلوماتي؛

- الاستيلاء على البيانات؛

- الاحتيال المعلوماتي؛

- اتلاف وتدمير البيانات.

• الهيئة الوطنية للوقاية ومكافحة الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال: من خلال المرسوم الرئاسي 15-261 المؤرخ في 08 اكتوبر 2015 (بركان و رملي، 2024) ؛

• القانون 06-22: يقتضي بالتحقيق في الجرائم الالكترونية و ذلك من خلال اعتراض و مراقبة المواصلات الالكترونية و تسجيلها اذا اقتضى الامر (قطاف و بوقرين، 2023، صفحة 86).

2.2.4 هيئات الامن السيبراني الجزائرية: قصد تدارك متطلبات الامن السيبراني لجأت الدولة الى

تشكيل عدة هيئات في هذا الخصوص:

• الهيئة الوطنية الخاصة بالوقاية و مكافحة الجرائم ذات الصلة بتكنولوجيا الاعلام و الاتصال:

اسست بموجب مرسوم رئاسي رقم 19-172 سنة 2019، و هي هيئة توضع تحت سلطة وزارة

الدفاع الوطني تختص بالمراقبة الوقائية للاتصالات لمكافحة الجرائم المعلوماتية التي تمس الدولة (بوزيرة،

2022، صفحة 562)؛

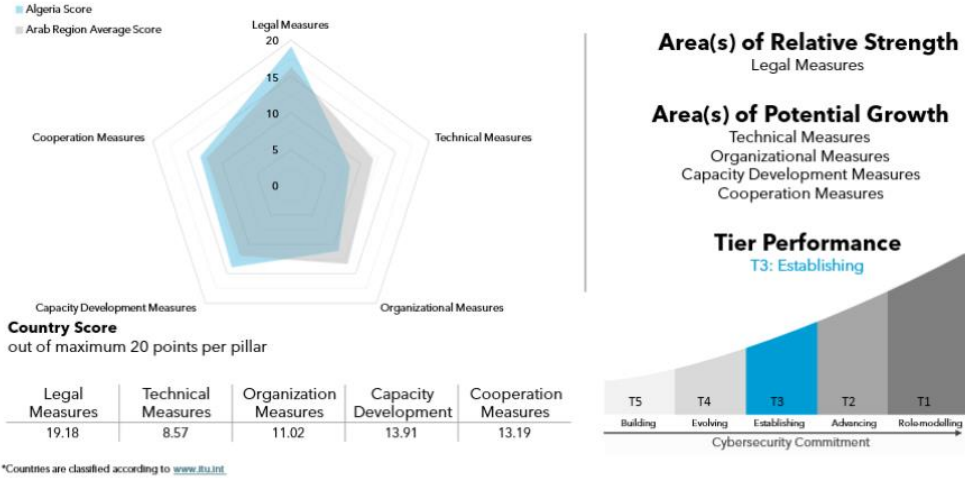
- مركز الوقاية من الجرائم المتصلة بالإعلام الالي و الجرائم المعلوماتية (الدرك الوطني): انشئ سنة 2008، يسعى الى تأمين منظومة المعلومات لخدمة الامن العمومي من خلال معالجة و تحليل معطيات بيانات الجرائم المعلوماتية المرتكبة و ضمان الرقابة المستمرة على الانترنت و مراقبة مراكز و جهات الاتصال الالكترونية بما يخول له القانون (بلقاسم و بوشوشة، 2023، صفحة 552)؛
- المصلحة المركزية لمكافحة الجريمة المعلوماتية (مديرية الامن الوطني): انشئت بهدف مكافحة الجريمة الالكترونية و يمتد نشاطها الى التنسيق الدولي مع هيئات الامن السيبراني الدولية (زمورة و بن عيسى ، 2022، صفحة 424)؛
- المعهد الوطني للأدلة الجنائية و علم الاجرام (الدرك الوطني): انشئ بموجب المرسوم الرئاسي رقم 04-183 المؤرخ في 26 جوان 2004، تتمثل مهامه في اجراء الخبرات و الفحوصات المطلوبة من طرف القضاة و المحققين في اطار التحريات اللازمة و يشارك في الدراسة و التحاليل و تصميم المعطيات القانونية (بلقاسم و بوشوشة، 2023، صفحة 550).

3.2.4 البنوك العمومية الجزائرية في تحدي حوكمة الامن السيبراني:

الشكل 01: الامن السيبراني في الجزائر

Algeria

GCI 5th Edition Country Profile



المصدر: (International Telecommunication Union, 2024, p. 70)

أعرب الاتحاد الدولي للاتصالات في إصداره الخامس لسنة 2024، على أن الجاهزية السيبرانية

للجزائر تصنف على عدة محاور بالنسبة للمجموعة العربية:

- التدابير القانونية: تسجل تقدم ملحوظ 20/19.18
- التدابير التقنية: 20/8.57 و هو ما يترجم أداء ضعيف مقارنة بالدول الأخرى
- التدابير التنظيمية : 20/10.2 معدل متوسط
- تدابير تنمية القدرات: 20/9.67 و هو معدل أقل من المتوسط
- تدابير التعاون: 20/12.12 نسبة معتدلة نوعا ما
- تصنيف الجاهزية السيبرانية T2 : فئة المستوى المتوسط

عنوان المقال: حوكمة البنوك العمومية الجزائرية كآلية لإدارة مخاطر الامن السيبراني في ظل استخدامات الذكاء

الاصطناعي -دراسة حالة عينة من البنوك العمومية الجزائرية-

يمكن القول ان الجزائر اتخذت عدة اجراءات و تدابير سمحت لها بإحراز التقدمات السابقة الذكر،
الا انه عليها العمل أكثر على تعزيز التجهيزات التقنية و التنظيم المؤسساتي و التعاون الدولي في مجال الامن
السيبراني.

الجدول 02: حوكمة الامن السيبراني بالبنوك العمومية الجزائرية

البنك	CNEP	BEA	BNA	CPA	BADR
مؤشر الحوكمة	توجد	استراتيجية حماية متقدمة (حماية الوصول من خلال الامن على مستويين باستعمال الهاتف الشخصي)	توجد	توجد	توجد
استراتيجية الامن السيبراني بالبنك (دور مجلس الادارة بضبط و اعتماد استراتيجية واضحة المعالم للأمن السيبراني و تطبيقها)					

انشاء ادارة (مصلحة) خاصة بالأمن السيبراني في البنك	توجد مصلحة الاعلام الالي، تقوم بمهام الامن السيبراني	موجودة على مستوى الإدارة العامة	على مستوى الإدارة العامة	مديرية خاصة بالأمن السيبراني على مستوى الإدارة العامة	على مستوى الإدارة العامة مع متابعة دورية للوكالات
الافصاح عن المخاطر السيبرانية (الافصاح الدوري)	افصاح داخلي (بين الوكالة والإدارة العامة)	يوجد	افصاح داخلي	لا يتم الا اذا طلب البنك المركزي ذلك (حفاظا على السرية والسمعة)	يتم على مستوى الإدارة العامة
المساءلة	مراقبة مستمرة لأداء الموظفين و المساءلة في حال اللزوم	تفرض المساءلة من طرف الإدارة العامة	مساءلة عند الاقتضاء	عند الاقتضاء	مساءلة من طرف الإدارة العامة و الإدارة الاقليمية
كفاءة نظام الرقابة الداخلية و التدقيق (لجان المراجعة)	لجان تدقيق داخلية تسهر على الامتثال لقوانين الامن السيبراني	لا توجد	توجد	توجد	توجد

التوعية و التدريب للموظفين+ العملاء	توعية مستمرة للموظفين فقط،(تعليمات مستمرة من الإدارة العامة، تكوين في جديد الامن السيبراني، أبواب مفتوحة)	أيام تحسيسية أبواب مفتوحة تكوين	-تكوين من طرف الإدارة العامة -أيام تحسيسية -أبواب مفتوحة - مراسلات متواصلة	تكوين - من طرف الإدارة العامة أيام - تحسيسية أبواب - مفتوحة -مراسلات متواصلة	تكوين - من طرف الإدارة العامة أيام - تحسيسية -أبواب مفتوحة
المراجعة الدورية لضوابط الامن السيبراني المقدمة من طرف السلطات الاشرافية و الرقابية المحلية	تقارير ربع سنوية حول الامن السيبراني و المخاطر السيبرانية التي تعرض لها البنك	توجد	توجد	تواصل مستمر و تنفيذ تعليمات الوكالة الوطنية للأمن السيبراني	توجد

المصدر: من اعداد الباحثين، اعتمادا على معطيات الدراسة الميدانية

تبدي البنوك الجزائرية اهمية بالغة للأمن السيبراني و هو ما يظهر جليا من خلال التدابير المتخذة من اجل حوكمته و ادارة المخاطر السيبرانية بها، حيث اعربت اغلبية البنوك عن اتخاذ سياسة واضحة

بشان حوكمة الامن السيبراني و الاستعانة بمزودي خدمات خارجيين لدعم الامن بمصالح البنوك، و تعزيز ممارسات حماية الانظمة :

- تمارس حماية أنظمة المعلومات على عدة مستويات بالنسبة لكل الموظفين من اجل الوقاية و الحماية ضد أي تهديد؛
- يتلقى رؤساء المصالح بشكل دوري توجيهات و تعليمات بخصوص الامن السيبراني من طرف الإدارة العامة، و هو ما يعكس التزام البنوك إرساء قواعد و اليات الحوكمة السيبرانية؛
- تبدي البنوك استجابة لمتطلبات الحوكمة السيبرانية المقدمة من طرف الهيئة الوطنية للأمن السيبراني؛
- توعية و تكوين الموظفين في مجال الامن السيبراني؛

ادى هذا الالتزام الى محاربة المخاطر السيبرانية و الحد منها في البنوك العمومية الجزائرية، الا انه تم تسجيل بعض النقائص:

- نقص الاهتمام بتوعية العملاء بالأمن السيبراني؛
- وجود مصالح الامن السيبراني على مستوى الإدارات العامة فقط؛
- الغياب شبه التام للبنك المركزي بخصوص الامن السيبراني وإرساء حوكمته.

5. خاتمة:

رغبة و ارادة الجزائر في رقمنة القطاع المصرفي مدعوما بحوكمة الامن السيبراني، دفع البنوك العمومية الجزائرية الى مواكبة التطور التكنولوجي واستخدامات الذكاء الاصطناعي، حيث التزمت البنوك بإصدار خدمات رقمية جديدة و تحديث انظمتها بما يتماشى والتطورات العالمية و رغبات و تطلعات العملاء، و هو ما يعكس النتائج التالية:

- تكيف البنوك العمومية الجزائرية مع التطورات العالمية في اصدار الخدمات الرقمية؛
- دعم حوكمة الامن السيبراني في البنوك الجزائرية كآلية للحماية من المخاطر السيبرانية؛
- حوكمة الامن السيبراني في البنوك احرزت نتائج ايجابية في الحماية من المخاطر السيبرانية؛
- تجاهل عامل تثقيف العملاء في مجال الامن السيبراني؛
- غياب مراقبة البنك المركزي للبنوك فيما يخص الامن السيبراني.

من خلال النتائج السابقة، يمكن ابداء بعض التوصيات:

- تعزيز حوكمة الامن السيبراني بالبنوك العمومية والاستفادة من التجارب الدولية في المجال؛
- الحرص على متابعة ومرافقة من طرف البنك المركزي وذلك من خلال انشاء اطار واضح لحوكمة الامن السيبراني؛
- إلزام الجهات الرقابية والاشرفية بمتابعة دورية للتحقق من مدى تنفيذ برنامج حوكمة الامن السيبراني بالبنوك؛

6. قائمة المراجع :

- 1.Almohri, H. (dec 2024). *Governance of Cybersecurity in Banking and Financial Organizations*. Institute of Banking Studies Research.
- 2.AUTORITE DES MARCHES FINANCIERS. (2024, 02 01). Consulté le 03 06, 2025, sur AMF-France.Org: <https://www.amf-france.org/fr/actualites-publications/actualites/cybersecurite-et-risques-informatiques-lamf-appelle-les-acteurs-se-preparer-lentree-en-application>
- banque d'algérie .(2005) .3.reglement N°2005-06 du 15/12/2005 portant sur la compensation des cheques at autres instruments de paiement de masse .banque d'algérie.
- 4.Basel Committee on Banking Supervision. (2023). *Core principles for effective banking supervision*. Bank for International Settlements.
- 5.cyber management school. (2024, 04 03). Consulté le 03 02, 2025, sur Cyber Management School: <https://www.cyber-management-school.com/actualite/les-banques-face-aux-risques-des-cyberattaques/>
- 6.International Telecommunication Union. (2024). *Global Cybersecurity Index 2024 5th Edition*. ITU Publications.
- 7.Jean, M., & Viviane , N. (2016). *Gouvernance des organisations Exemples sectoriels enjeux transverses*. 11 rue Paul Bert, 92240 Malakoff: DUNOD.
- 8.Léa, M. (2023, 12 23). *blog metiers*. Consulté le 03 01, 2025, sur freelance.com:

<https://www.freelance.com/blog/metiers/cybersecurite-banques-assurances/>

9.Linna, L. (2024, 11 29). Consulté le 03 04, 2025, sur paperjam.lu: <https://paperjam.lu/article/risque-lies-a-cybersecurite-au-coeur-des-priorites/>

10.Securities and Exchange Commission (SEC). (2022). Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure. Consulté le 03 03, 2025, sur SEC: <https://www.sec.gov/corpfin/secg-cybersecurity>

S.11&P Global Ratin (2024). الاستعداد الدائم عامل حاسم لمواجهة المخاطر السيبرانية لدى البنوك الخليجية.

12. احمد رجب عبد العظيم. (2024). استخدام الذكاء الاصطناعي في تعزيز الامن السيبراني في البنوك. بحث مقدم ضمن المسابقة البحثية للمركز الاعلامي العربي بالتعاون مع المعهد المصري لعام 2024 حول موضوع "استخدام الذكاء الاصطناعي في تعزيز الامن السيبراني بالبنوك".

13. اكرام بركان، و فهم رمللي. (2024). واقع و اشكالات الامن السيبراني في الجزائر. ورقة بحثية مقدمة للمؤتمر العلمي الوطني الأول حول "الاستراتيجية الجائزة الكبرى لتحقيق أهداف الأمن الشامل و التنمية المستدامة" يومي 31-31 فيفري 2021 بكلية العلوم السياسية ، جامعة صالح بونيدر قسنطينة 3.

14. إيمان فنيش، و حياة نجار. (2024). ابتكارات التكنولوجيا المالية كتوجه لتطوير الخدمات المصرفية الإلكترونية في البنوك التجارية دراسة حالة البنك الوطني الجزائري. مجلة أبحاث إقتصادية معاصر، المجلد 07، العدد 01.

15. بن جدو بن علي. (2022). تحديات الامن السيبراني لمواجهة الجريمة الالكترونية. المجلة الجزائرية للامن الانساني، المجلد 07، العدد 02.

16. بنك الجزائر. (2024). نظام رقم 02-24 مؤرخ في 13 أكتوبر 2024، يتعلق بالشروط الخاصة لترخيص بتأسيس و اعتماد و ممارسة نشاط البنك الرقمي. الجزائر: بنك الجزائر.

17. جمال زمورة ، و ليلي بن عيسى . (2022). أهمية حوكمة الأمن السيبراني لضمان تحول رقمي آمن للخدمات العمومية في الجزائر. مجلة البحوث الاقتصادية المتقدمة، المجلد 07، العدد 02.

18. جميلة جغل، و عادل زقير. (2023). الأمن السيبراني والشمول المالي في ظل التحول الرقمي للقطاع المالي (التحديات السيبرانية، البات التحوط). مجلة التنمية الاقتصادية، المجلد 08، العدد 01.

19. حاكم محسن الربيعي، و حمد عبد الحسين راضي. (2020). حوكمة البنوك و اثرها في الاداء و المخاطرة . كربلاء، العراق: اليازوري للنشر و التوزيع.
20. حفيظة كراع. (2021). العمل المصرفي الالكتروني و المسؤولية المدنية للبنك فيه . باتنة: جامعة باتنة 01 الحاج لخضر كلية الحقوق و العلوم السياسية قسم الحقوق. اطروحة مقدمة لنيل شهادة الدكتوراه في الحقوق.
21. حفيظة كراع، و مريم ناي. (11 ديسمبر 2024). الصيرفة الالكترونية في الجزائر قراءة للقانون النقدي و المصرفي 09-23. مداخلة مقدمة ضمن فعاليات الملتقى الوطني الموسوم بعصرنة القطاع المصرفي الجزائري-واقع و افاق- جامعة الجزائر 1 يوسف بن خدة، كلية الحقوق، 313.
22. ساعد بوقرص. (2022). الأمن السيبراني: مخاطر و تهديدات و تحديات تتطلب ممارسات و توصيات واستراتيجيات خاصة. مجلة الأبحاث في الحماية الاجتماعية، المجلد 03، العدد 01.
23. سليمان قطاف، و عبد الحليم بوقرين. (2023). الآليات الموضوعية و الاجرائية المتبعة لتحقيق الامن السيبراني الجزائر نموذجا. مجلة الحوكمة و القانون الاقتصادي، المجلد 03، العدد 02.
24. سميحة بلقاسم ، و حميد بوشوشة. (2023). الجريمة الالكترونية بعد جديد للجرائم في الجزائر واقعها و البات مجابتهها . مجلة العلوم الانسانية لجامعة ام البواقي، المجلد 10، العدد 01.
- في الجزائر السياسات و المؤسسات. المجلة 25Cyber Security. سمير بارة. (2017). الامن السيبراني الجزائرية للامن الانساني، العدد 04.
26. سهيلة بوزيرة. (2022). الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال بين سرية المعطيات الشخصية الالكترونية و مكافحة الجرائم الالكترونية. المجلة النقدية للقانون و العلوم السياسية، المجلد 07، العدد 02.
27. شريف علي خميس ابراهيم كعموش. (2024). أثر بدائل إفصاح البنوك عن إدارة مخاطر الأمن السيبراني على أحكام عملائها والمستثمرون في أسهمها: دراسة تجريبية. مجلة البحوث المحاسبية، المجلد 11، العدد 03.
28. صندوق النقد الدولي. (2024). تقرير الاستقرار المالي العالمي.
29. صندوق النقد العربي اللجنة العربية للرقابة المصرفية. (2017). مبادئ حوكمة المؤسسات المصرفية، ورقة محدثة رقم 73. أبو ظبي: أمانة محافظي المصارف المركزية و مؤسسات النقد العربية.

30. فتيحة حزام . (2020). حماية الانظمة الرقمية بين الاليات التقنية و اجهزة الحماية قراءة في احكام المرسوم الرئاسي 05-20. مجلة الحقوق و العلوم الانسانية، المجلد 13، العدد 03.
31. محمد اسماعيل. (2019). الأمن السيبراني في القطاع المصرفي، موجز سياسات: العدد 04. صندوق النقد العربي.
32. محمد حارس محمد طه ابو الخير. (2023). أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية (دراسة ميدانية). المجلة العلمية للدراسات والبحوث المالية والإدارية، المجلد 15، العدد 01.
34. مختار رنان. (2023). الجيل الثالث من الإصلاحات النقدية والمصرفية في الجزائر قراءة في مضمون القانون 09-23. مجلة ابحاث اقتصادية معاصرة، المجلد 06، العدد 01.
35. مروة فتحى السيد البغدادى. (2021). اقتصاديات الامن السيبراني في القطاع المصرفي. مجلة البحوث القانونية و الاقتصادية، العدد 76.
36. مصطفى بن شلاط. (2022). واقع الصيرفة الالكترونية و وسائل الدفع في الجزائر. مجلة البشائر الاقتصادية، المجلد 08، العدد 01.