مساهمة الأمن المعلوماتي في تفعيل الصيرفة الإلكترونية -حالة الجزائر-

The contribution of information security to the activation of electronic banking -Algeria case-

ط.د. هاجر بديرينة[1]* أ.د مصطفى بورنان

[1] مخبر دراسات التنمية الإقتصادية، جامعة عمار الثليجي -الاغواط، (الجزائر)، h.bederina@lagh-univ.dz

تاريخ الاستلام: 2022/12/21 تاريخ القبول: 2022/12/30 تاريخ النشر: 2023/01/05

ملخص:

تهـدف هـذه الدراسـة إلى تسـليط الضـوء حـول الأمـن المعلومـاتي و مسـاهمته في تفعيـل الصـيرفة الإلكترونيـة لاسـيما مع بـروز الرقمنـة و مدى إسـتخدام وسـائل تكنولوجيـا المعلومـات و الإتصـال في المصـرف في حد ذاته، و تستمد هذه الدراسة أهميتها من خلال إبراز مكانة الامن المعلوماتي في حماية الصيرفة الإلكترونية أمام التهديدات المختلفة بإتخاذ مختلف التدابير الرامية للحفاظ على المعلومات و الأجهزة و الأنظمة من كل عملية قرصنة قد تحدث بصفة غير قانونية سواءا من داخل القطاع أو خارجه، و عليه توصلت الدراسة إلى أن هناك علاقة تكاملية تجمع بينهما فكلما كان الأمن المعلوماتي متوفر كلما كانت الصيرفة الإلكترونية أكثر فعالية، و دولة الجزائر تشهد تطورا نسبيا قد لا يرقى إلى المستوى المطلوب و لكنه لبنة أساسية تساهم في ترقية العمل المصرفي الإلكتروني.

الكلمات المفتاحية: الأمن المعلوماتي؛ الصيرفة الإلكترونية؛ تكنولوجيا المعلومات و الإتصال.

تصنيف JEL: G21، E59، O32

Abstract:

This study aims to shed light on information security and its contribution to activating electronic banking, especially with the emergence of digitization and the extent to which the means of information and communication technology are used in the bank itself. By taking various measures aimed at preserving information, devices and systems from every piracy process that may occur illegally, whether from inside or outside the sector.

Accordingly, the study concluded that there is an integrative relationship that brings them together, the more information security is available, the more effective the electronic banking, and the state of Algeria is witnessing a relative development that may not rise to the required level, but it is a basic building block that contributes to the promotion of electronic banking.

Keywords:information security; electronic banking; Information and communication technology

Jel Classification Codes: G21,E59,O32

*المؤلف المرسل: هاجر بديرينة

1. مقدمة:

لقد أتاح التطور المذهل الذي شهده قطاع التكنولوجيا المالية الكثير من الفرص أمام المصارف لتحسين مستوى الخدمات المقدمة للعملاء من خلال قنوات جديدة و مبتكرة، مما أدى إلى بروز المصارف الإلكترونية إلى حيز الوجود لكن سرعان ماصطدمت هذه المصارف بالمشاكل التكنولوجية أو الجرائم المعلوماتية و أصبح من الضروري البحث عن الحلول لهذه المشاكل من خلال إتخاذ التدابير الرامية للحفاظ على المعلومات و الأجهزة و البرمجيات و... من كل عملية قرصنة قد تحدث بصفة غير قانونية و هو ما أصطلح على تسميته بتوفير الأمن المعلوماتي الذي يعتبر من بين المسائل الهامة التي تطرح نفسها في الآونة الأخيرة لما تشهده المعاملات الإلكترونية بصفة عامة من حركية واسعة و المجال المصرفي و المالي على وجه الخصوص، و من خلال هذا إرتاينا طرح الإشكالية الرئيسية التالية:

كيف يساهم الأمن المعلوماتي في تفعيل الصيرفة الإلكترونية؟

و للإجابة على هذا التساؤل تم طرح الفرضية الرئيسية المتمثلة في:

يساهم الأمن المعلوماتي في تفعيل الصيرفة الإلكترونية من خلال تأمين و حماية معلوماتها و أنظمتها و وسائطها من وصول غير المصرح لهم سواء لمن هم داخل القطاع أو خارجه.

الهدف من الدراسة:

تهدف هذه الدراسة إلى التعرف على الصيرفة الإلكترونية و الأمن المعلوماتي و معرفة العلاقة التي تجمع بينهما، و ذلك من خلال عرض الأليات و الميكانزمات و إسقاطها على دولة الجزائر.

أهمية الدراسة:

تكمن أهمية الدراسة في تناولها لموضوع الأمن المعلوماتي و الذي أصبح له دور مهم في تفعيل الصيرفة الإلكترونية أمام التهديدات المختلفة بإتخاذ مختلف التدابير الرامية للحفاظ على المعلومات و الأجهزة و الأنظمة من كل عملية قرصنة قد تحدث بصفة غير قانونية.

منهجية الدراسة:

لتحقيق هدف الدراسة تم الإعتماد على المنهج الوصفي التحليلي لكونه ملائما لعرض المفاهيم المتعلقة بموضوع الدراسة و ذلك من أجل تجميع المعلومات و الحقائق المتعلقة بالموضوع ثم تحليلها ثم تبويبها للوصول إلى معرفة تفصيلية بالموضوع.

2. الصيرفة الإلكترونية، أنظمة دفعها و جرائمها الإلكترونية

قبل التعرف على وسائل الدفع الإلكترونية يجب أولا تقديم تعريف حول الصيرفة الإلكترونية.

1.2 تعريف الصيرفة الإلكترونية:

هي تقديم الخدمات المصرفية بإستعمال تكنولوجيات المعلومات و الإتصال أي من خلال الإنترنيت و الموزعات الألية و الشبكات الخاصة و الهاتف النقال و الثابت و الحاسب الشخص فهي تتيح الخدمة المصرفية عن بعد و خلال 24 ساعة و كل أيام الأسبوع و بسرعة فائقة و بتكلفة أقل و بدون إلتقاء مكاني بين العميل و المصرف. (بوعافية و زويتة، 2010، صفحة 145)

2.2 تعريف أنظمة الدفع الإلكترونية

تعرف على أنها الوسيلة التي تمكن صاحبها من القيام بعمليات الدفع المباشر عن بعد عبر الشبكات العمومية للإتصالات.

تعرف على أنها أنظمة الدفع التي تتم إلكترونيا بدلا من ورق الكشف أو البيانات و يمكن الشخص من محاسبة فواتيره إلكترونيا أو القيام بتحويل النقود إلكترونيا عبر حسابه البنكي الخاص. (عريوة و خاوي، 2017، صفحة 141)

3.2 أنواع أنظمة الدفع الإلكترونية

تعددت وسائل الدفع الإلكترونية و إتخذت أشكالا تتلاءم و متطلبات التجارة الإلكترونية و كذلك طبيعة المعاملات عبر شبكة الإنترنيت و كانت بدايتها بظهور البطاقات البنكية و التي طورت فيما بعد من البطاقات ذات الشريط المغناطيسي إلى البطاقة ذات الخلية الإلكترونية كما ظهرت وسائل دفع إلكترونية أخرى و فيما يلي تفصيلها: (عريوة و خاوي، 2017، الصفحات 141-143)

- **البطاقات البنكية:**

تعرف البطاقات البنكية على أنها بطاقات بلاستيكية و مغناطيسية يصدرها البنك لصالح عملائه بدلا من حملهم للنقود، شكلها مستطيلي تحمل إسم الجهة المصدرة لها شعارها و توقيع حاملها و بشكل بارز على وجه الخصوص رقمها و إسم حاملها و رقم حسابه و تاريخ إنتهاء صلاحيتها، تستخدم هذه البطاقات في السحب النقدي من الآت الصراف الآلي(**ATM**) و في شراء السلع و الخدمات حيث تعطي لحاملها قدرا كبيرا من المرونة في السداد و قدر أكبر من الأمان و تكلفة أقل في إتمام العمليات و بسرعة أكبر في إتمام التسويات المالية.

- **البطاقات الذكية:** و هي عبارة عن بطاقة بلاستيكية ذات حجم قياسي تحتوي على شرائح للذاكرة تعمل بواسطة ميكرو كمبيوتر يزودها ببطاقة تخزينية للبيانات تفوق بكثير تلك التي تستوعبها البطاقات ذات الشرائط الممغنطة بالمقابل فهي أعلى منها تكلفة و تقدم هذه

البطاقات العديد من الخدمات للعميل مثل البيانات الشخصية لحاملها و كذا معلومات عن حساباته المصرفية و بإستخدام البطاقة في الحاسوب الشخصي أو في أجهزة الصراف الآلي، يمكن للعميل شحنها بمبلغ معين من النقود إنطلاقا من حسابه فهي لا تعتمد على الإتصال من حاسوب المصرف المصدر لها بل تعتبر بمثابة كمبيوتر متنقل و تمثل حماية عالية ضد التزوير و سوء الإستخدام كما تتيح لأجهزة قراءة البطاقات التي توضع بالمحلات التجارية التدقيق في تفاصيل الحسابات المالية لصاحبها.

- **النقود الإلكترونية:**

عرفها البنك المركزي الأوربي بأنها:" مخزن إلكتروني لقيمة نقدية على وسيلة تقنية يستخدم بصورة شائعة للقيام بمدفوعات لمتعهدين من غير من أصدرها دون الحاجة إلى وجود حساب بنكي عند إجراء الصفقة و تستخدم كأداة محمولة مدفوعة مسبقا".

- **المحافظ الإلكترونية:**

المحافظ الإلكترونية تقوم بتحويل النقد إلى سلسلة رقمية و تخزن على القرص الثابت في أماكن العمل للحد من إستخدام النقود في المعاملات التي تتم على شبكة الإنترنيت و معظم الحقائب الإلكترونية تقوم بتخزين النقد الإلكتروني على البطاقات الذكية التي تتمكن من دفع أي مبلغ من الحقيبة الإلكترونية في أي مكان.

- **الشيكات الإلكترونية:**

الشيكات الإلكترونية مثل الشيكات التقليدية تتضمن أمر بالدفع من الساحب إلى المسحوب عليه لدفع مبلغ معين إلى المستفيد غير أن الإلكترونية تختلف في أنها ترسل إلكترونيا، و بعبارة أخرى الشيك الإلكتروني هو رسالة إلكترونية موثقة و مؤقتة يرسلها مصدر الشيك ليعتمده و يقدمه للبنك الذي يعمل عبر الإنترنيت ليقوم هذا الأخير بتحويل قيمة الشيك المالية إلى حساب حامل الشيك ليتم بعد ذلك إلغاء الشيك و إعادته إلكترونيا إلى مستلم الشيك ليكون دليلا على أنه تم صرف الشيك فعلا و يمكن لمسلم الشيك أن يتاكد إلكترونيا من أنه قد تم فعلا تحويل المبلغ لحسابه.

- **التحويلات المالية الإلكترونية:** يهدف هذا النظام إلى تسهيل المدفوعات و التسويات بين المصارف و يكفل هذا النظام للمصارف المحلية قدرة تقديم خدمات أفضل للعملاء إذ يتيح

لها إمكانية التسوية الفورية من دفع و تلقي الأموال عبر حساباتها الجارية لدى المصارف المركزية و كذا توفير دفع فوري لعملائها.

4.2 الجرائم المعلوماتية في الصيرفة الإلكترونية

تعد جريمتي القرصنة و غسيل الأموال من أكبر الجرائم المعلوماتية التي تخلف خسائر هامة في القطاع المصرفي.

- **جريمة القرصنة:**

و يقصد بها تزوير بطاقات الإئتمانية البنكية و ذلك عن طريق التوصل إلى معرفة الأرقام السرية لهذه البطاقات و التي يتم إكتشافها بتقنيات مختلفة كسرقة المعلومات التي يحويها العقل المغناطيسي لهذه البطاقات من طرف العاملين بالفنادق و المحلات لحظة أداء المستهلكين لهذه البطاقات لفواتير إستهلاكهم أو قراءة المعلومات التي تتضمنها العقل المغناطسي بواسطة أجهزة و آلات للقراءة و نقل هذه المعلومات و طبعها في بطاقات بيضاء فارغة بواسطة آلات و أجهزة للكتابة و الطبع. كما أن هذه النقود معرضة إلى السرقة من خلال الدخول غير المشروع إلى أجهزة و أنظمة الحساب الشخصي المحفوظة على جهاز الكمبيوتر عن طريق ما يعرف بتقنية فك التشفير غير المشروع.

- **جريمة تبيض الأموال:**

لقد ساهمت الأساليب التكنولوجية بشكل كبير في عملية إنتشار عمليات غسيل الأموال عبر البنوك و يمكن ذكر اهم هذه الأساليب فيمايلي:

- الخدمات المصرفية الإلكترونية؛
- بنوك الإنترنيت: هذه الأخيرة لا تقوم بدور البنوك التقليدية و إنما تعتبر وسيط لإنجاز بعض العمليات المالية عن طريق إدراج العميل للرقم السري في الكمبيوتر ليتم تحويل مباشرة الأموال بسرعة فائقة؛
- ظهور أنظمة تحويل إلكترونية مهمتها تحويل الأموال بين البنوك العالمية و أبرزها: **swift/chips**

وفقا لنظام سويفت يقوم البنك بتنفيذ التحويل و لا يعلم الغرض من عملية التحويل فالبنك المصرح هو وحده الذي يقع عليه واجب التحري عن غرض العميل من هذا الإستخدام و عليه فإن التحويلات

الصادرة من البنوك الأجنبية غالبا ما تكون خيالية من إسم العميل المنشأ إذ تقتصر على ذكر عبارة "أن عميلنا يرغب في تحويل... إلى عميلكم". (قارة، 2016، الصفحات 419-421)

و عليه فإن خطر الجرائم الإلكترونية و الجماعات الإجرامية المتخصصة بتزوير البيانات و سرقة المعلومات الشخصية هو أكثر ما يقلق القطاعات المصرفية عند إستعمالها للتقنيات المستجدة، لهذا يستدعي حماية أنظمة الدفع الإلكترونية من خلال الأمن المعلوماتي لحماية و سلامة هذه التعاملات.

3. دور الأمن المعلوماتي لحماية الصيرفة الإلكترونية

تشكل المعلومات المصدر الأساسي الذي يتيح للمنظمات إتخاذ القرارات المناسبة و يمكنها من تأدية مهامها إذ أن نوع المعلومات و كميتها و طريقة عرضها تعتبر الأساس في نجاح عملية صنع القرارات داخل المنظمات المعاصرة و عليه فإن للمعلومات قيمة عالية تستوجب وضع الضوابط اللازمة لإستخدامها و تداولها و وضع السبل الكفيلة بحيازتها لذا فإن المشكلة التي يجب أخذها بالحسبان هو توفير الحماية اللازمة للمعلومات و إبعادها عن الإستخدام غير المشروع لها.

1.3 التعريف بالأمن المعلوماتي: من ضمن التعاريف التي أعطيت للأمن المعلوماتي نجد:

يعرف أمن المعلومات من زاوية أكاديمية بأنه العلم الذي يبحث في نظريات و إستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها و من أنشطة الإعتداء عليها، و من زاوية تقنية هو الوسائل و الأدوات و الإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية و الخارجية (الشمالي، 2017، صفحة 189)، ومن زاوية قانونية فإن أمن المعلومات هو محل دراسات تدابير حماية سرية و سلامة محتوى و توافر المعلومات، مكافحة أنشطة الإعتداء عليها، أو إستغلال نظمها في إرتكاب الجريمة (بن قارة، 2021، صفحة 28)، كما يشير أيضا إلى كل موارد المعلومات المنظمة من السرقة من قبل أطراف غير مخول لها إستخدام النظام. (زيدان و حمو، 2015، صفحة 163)

يعرف على أنه مجموعة من الإجراءات و التدابير الوقائية التي تستعمل سواء في المجال الفني او الوقائي لصيانة المعلومات الخاصة بالإدارة الإلكترونية و الإجراءات القانونية التي تتخذ لتحمي من حدوث أي تدخلات غير مشروعة سواء عن طريق الصدفة أو بشكل متعمد. (حمودي، 2020، صفحة 95)

يعرف بأنه ذلك الحقل الذي يهتم بدراسة طرق حماية البيانات المخزنة في أجهزة الحواسيب و الأجهزة الملحقة و شبكات الإتصالات و التصدي للمحاولات الرامية إلى الدخول غير المشروع إلى قواعد البيانات المخزنة أو تلك التي ترمي إلى نقل أو تغيير أو تخريب تلك المعلومات. (بربار و قلمين، 2014، الصفحات 14-15)

فمن خلال ماسبق يمكن أن نعرف الأمن المعلوماتي بأنه مجموعة من العمليات و الإجراءات و الأدوات التي تتخذها القطاعات أو المنظمات لتأمين و حماية معلوماتها وأنظمتها و وسائطها من وصول غير المصرح لهم، سواء لمن هم داخل القطاع أو خارجه.

2.3 عناصر الأمن المعلوماتي: يتكون الأمن المعلوماتي من أربعة عناصر رئيسية تتمثل في: (حمودي، 2020، الصفحات 96-97)

- **السرية أو الموثوقية:** و تعني التأكد من أن المعلومات لا تكشف و لا يطلع عليها من قبل أشخاص غير مخولين بذلك؛
- **التكاملية وسلامة المحتوى:** التأكد من أن محتوى المعلومات صحيح و لم يتم تعديله، أو العبث به؛
- **إستمرارية توفر المعلومات أو الخدمة:** التأكد من إستمرار عمل النظام المعلوماتي و إستمرار القدرة على التفاعل مع المعلومات، و تقديم الخدمة لمواقع المعلوماتية، و إن مستخدم المعلومات لن يتعرض إلى منع إستخدامه لها، أو دخوله إليها؛
- **عدم إنكار التصرف المرتبط بالمعلومات:** و يقصد به ضمان عدم إنكار الشخص الذي قام بتصرف ما متصل بالمعلومات أو مواقعها، أي أنه لا يمكن لأي طرف من الأطراف المشاركة في عملية التراسل إنكار القيام بالمعاملة أو الإجراء، و لضمان عدم النكران لا بد أن تتوافر إمكانية التتبع المستمر للمعاملة التي يتم القيام بها. (مريزق و بوقلاشي، 2010، الصفحات 12-13)

3.3 المخاطر التي تهدد الأمن المعلوماتي للصيرفة الإلكترونية و كيفية التعامل معها

- **المخاطر الداخلية:**

- **لامبالاة الموظفين:** إن إهمال المستخدم للنظام (موظف المصرف في هذه الحالة) يشكل أكبر تهديد للأمن المعلوماتي داخل المصرف، التي يمكن أن تحدث أثناء تصميم التجهيزات أو نظم

المعلومات أو خلال عمليات البرمجة أو الإختيار أو التجميع للبيانات أو أثناء إدخالها إلى النظام أو في عمليات تحديد الصلاحيات للمستخدمين و تشكل هذه الأخطاء الغالبية العظمى للمشاكل المتعلقة بأمن و سلامة نظم المعلومات في المنظمات. (القحطاني، 2003، صفحة 10)

- **الإحتيال و السرقة:** يشكل تحايل بعض الموظفين من داخل المصرف أعباء مالية كبيرة تخسر الشركات بمعدل 5 بالمئة من أرباحها السنوية نتيجة الإحتيال الداخلي بحسب إحصاءات جمعية ممتحني الإحتيال المعتمدين الـ AFCE ، و يوضح الشكل الموالي أنواع الإحتيال الداخلية التي تواجه حاليا فرق أمن المعلومات في القطاع المصرفي. (امن المعلومات في القطاع المصرفي المخاطر و التحديات، 2018)

الشكل 1: أنواع الإحتيال الداخلية التي تواجه حاليا فرق أمن المعلومات في القطاع المصرفي

source : https://www.ciatec.com

– **كيفية التعامل مع المخاطر الداخلية التي تهدد الأمن المعلوماتي للصيرفة الإلكترونية**

- **السياسات وسير الإجراءات الداخلية:** من الحكمة في البداية، إنشاء و توثيق سياسات و إجراءات واضحة المعالم، تكون بمثابة نقطة مرجعية مشتركة للفريق بأكمله. وجود هذه الوثائق سيمهد طريقة واضحة لضمان وجود التوحيد و التناسق في الممارسات و العمليات المعتمدة في مرحلة التشغيل؛
- **حملات توعية مستمرة حول أهمية أمن المعلومات في المصارف:** يجب أن تكون حملات التوعية دائمة التحديث و موجهة بشكل دوري لجميع العاملين داخل المصرف كأن يحسن الموظف التصرف مع الحوادث الأمنية داخل الشبكة؛
- **فحص الخلفية الجنائية و الوظيفية:** يجب أن يكون فحص الخلفية الجنائية و الوظيفية من الخطوات البديهية أثناء مرحلة التوظيف في أي مصرف؛

- **تدابير الأمن المادي في مراكز البيانات:** يمكن القول أن مراكز البيانات ينبغي أن تكون محمية إلى أقصى حد ممكن من الكوارث الطبيعية، و الصدمات الكهربائية، و تسرب المياه، و الرطوبة المرتفعة، و درجات الحرارة المرتفعة، و الحرائق ... إلخ. و كل هذا ينطوي تحت بند الأمن المادي و الضوابط البيئية في مراكز البيانات ضمن برنامج أمن المعلومات في المصرف؛

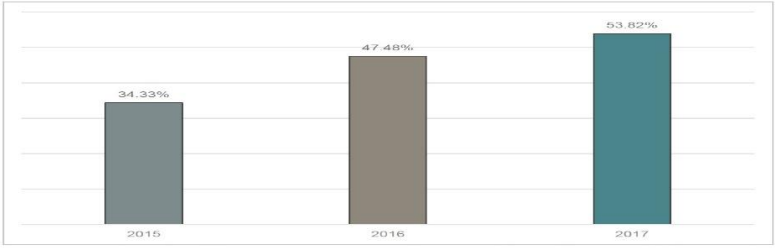
- **المصادقة و تفويضات الإستخدام:** وضع ضوابط التصريح بالدخول إلى المعلومات و تنفيذها و صيانتها بشكل دوري. (امن المعلومات في القطاع المصرفي المخاطر و التحديات، 2018)

– **المخاطر الخارجية**

- **التصيد الاحتيالي:** يقصد به الحصول على معلومات البطاقة المصرفية و كلمات المرور الخاصة بالحسابات المصرفية الإلكترونية؛

و يظهر الشكل أدناه من شركة كاسبرسكي لاب الروسية زيادة ملحوظة في حجم هجمات التصيد الإحتيالي على القطاع المصرفي بين عامي 2015 و 2017.

الشكل 2: حجم هجمات التصيد الإحتيالي على القطاع المصرفي الروسي



source : https://www.ciatec.com

- **هجمات على العملاء:** تجد المصارف في الترويج عبر الإنترنت حاجة متزايدة لضمان أمن معاملاتهم الرقمية و لكن حماية العميل لجهازه أو جواله هو على نفس القدر من الأهمية لأن أنظمة القرصنة تطبق قانون الغابة و تهاجم الفريسة الأضعف، أي جهاز العميل في حالتنا هذه؛ (امن المعلومات في القطاع المصرفي المخاطر و التحديات، 2018)

- **الجرائم المحوسبة:** تمثل هذه تحديا كبيرا لإدارة نظم المعلومات لما تسببه من خسارة كبيرة و بشكل عام يتم التمييز بين ثلاثة مستويات للجرائم المحوسبة و هي: (القحطاني، 2003، صفحة 10)

- سوء الإستخدام لجهاز الحاسوب و هو الإستخدام المقصود الذي يمكن أن يسبب خسارة للمصرف أو تخريب لأجهزته بشكل منظم؛
- سوء الإستخدام لجهاز الحاسوب و هو الإستخدام غير المقصود بشكل غير قانوني يؤدي إلى إرتكاب جريمة يعاقب عليها القانون خاصة بجرائم الحاسوب؛
- الجرائم التي تستخدم فيها الحواسيب كأداة لتنفيذ الجريمة.

و يمكن أن تتم الجرائم المحوسبة سواء من قبل أشخاص خارج المنظمة يقومون بإختراق نظام الحاسوب (غالبا من خلال الشبكات) أو من قبل أشخاص داخل المنظمة يملكون صلاحيات الدخول إلى النظام و لكنهم يقومون بإساءة إستخدام النظام لدوافع مختلفة.

– **كيفية التعامل مع المخاطر الخارجية التي تهدد الأمن المعلوماتي للصيرفة الإلكترونية**

- **الأمن المحيطي في القطاع المصرفي:** يشكل الأمن المحيطي خط الدفاع الأول ضد أي إختراق أمني، فهو يشكل حماية فعالة و يعتبر عنصرا أساسيا لإستراتيجية الأمن في المصارف و كثيرا ما يكون الجمع بين التكنولوجيا، الأمن المادي و تدريب الأفراد المعنيين أكثر الطرق فعالية للتكامل الأمني، مما يخلق طبقات دفاع متعددة لحماية محيط المصرف؛
- **مصادقة المستخدم و التصريح بالدخول:** بالنسبة للحسابات المصرفية إن الأولوية هي للأمن الإلكتروني لتصفح آمن عبر الإنترنت يجب البدء دائما بعملية المصادقة للتأكد من أن المستخدم هو المستخدم الصحيح المصرح له و ليس مقرصن أو سارق هوية، تتضمن المصادقة عموما مصادقة فردية و متعددة العوامل بالإضافة إلى تدابير" أمن الطبقات" (**Layered Security**) الإضافية عندما تقتضي الحاجة؛
- **المصادقة المتعددة العوامل (Multi-factor Authentication)**: تعتبر أساليب المصادقة التي تعتمد على أكثر من عامل واحد أكثر صلابة نظرا لصعوبة إختراق مصدرين للمصادقة في الوقت عينه و بناء على ذلك، فإن أساليب المصادقة متعددة العوامل المصممة و المطبقة بشكل صحيح أكثر موثوقية و رادعا أقوى من المصادقة القديمة التي تعتمد على إسم المستخدم و كلمة المرور فقط فمن المهم أن تتخذ المصارف الخطوات اللازمة لتنفيذ مصادقة متعددة العوامل آمنة؛

- **إدارة التصحيح (Patch Management)**: من الضروري وضع عملية إدارة التصحيح لضمان إتخاذ التدابير الوقائية المناسبة ضد التهديدات المحتملة، و التي تشمل أنظمة التشغيل و الخوادم و أجهزة التوجيه و أجهزة الحاسوب و عملاء البريد الإلكتروني و الأجهزة المحمولة و العديد من المكونات الأخرى الموجودة داخل البنية الأساسية للشبكة؛
- **توعية و تثقيف العملاء:** مما لا شك فيه أن تدريب و تعليم العملاء هو أحد الإجراءات الإحترازية الضرورية لحماية المعلومات السرية للعملاء، فتزويد العملاء بإرشادات عملية حول كيفية حماية أنفسهم من سرقة الهوية و الإحتيال الإلكتروني، و غيرها من التهديدات التي قد يواجهونها أثناء إستعمال الخدمات المصرفية عبر الإنترنت يساهم بشكل أساسي في التخفيف من تأثير الهجمات على العملاء التي ذكرناها سابقا؛
- **العمل مع أطراف ثالثة لتحسين الضوابط:** من المؤكد أن العمل مع أخصائي أمن المعلومات من مصادر خارجية كطرف ثالث هو طريقة ذكية لتحسين سير الأعمال ستوفر الوقت و الجهد على فرق أمن المعلومات داخل المصرف فيعطي الفريق فرصة للتركيز على العمليات الشاملة و تقديم أعلى مستويات الخدمة للمصرف و عملائها لكن أخذ الحيطة و الحذر مسألة واجبة و ضرورية لضمان إختيار أفضل الشركاء المحتملين، و ذلك لأن هناك دائما إحتمال لزيادة المخاطر الأمنية عند الإستعانة بمصادر خارجية. (امن المعلومات في القطاع المصرفي المخاطر و التحديات، 2018)

4.3 الأساليب التقنية لأمن المعلومات في الصيرفة الإلكترونية: نتعرض في هذا الصدد على سبيل المثال لا الحصر إلى التشفير، البصمة الإلكترونية، الجدار الناري، التوقيع الإلكتروني.

- **التشفير:**

يعرف التشفير على أنه :"آلية يتم بمقتضاها ترجمة معلومة مفهومة إلى معلومات غير مفهومة عبر تطبيق بروتوكولات سرية قابلة للإنعكاس، أي يمكن إرجاعها إلى حالتها الأصلية". (عيلام، 2018، صفحة 291)، و عادة ما يستند تشفير ملف ما إلى صيغة رياضية معقدة تسمى بالخوارزميات، و طول المفتاح (و الذي يقدر بالبت)، و بالتالي فك التشفير يكون عبارة عن إرجاع الملف المشفر إلى هيئته الأصلية، و هي صورة عن عملية تشفير ملف،و فك تشفيره، و طريقة التشفير هي تحويل المعلومات إلى أرقام و رموز يصعب فهمها من قبل الغير، و يكون ذلك باستخدام برامج خاصة للتشفير حيث تحول

هذه البرامج المعلومات إلى رموز و أرقام ضمن معادلة حسابية معينة، لا يمكن فهمها من قبل الغير إلا بإمتلاك البرنامج و الرقم السري لإعادة المعلومات إلى طبيعتها و يجري العمل بمثل هذه التقنية بأن يمتلك طرفا المعاملة البرنامج الخاص بالتشفير و ينقسم التشفير إلى تشفير متماثل و تشفير غير متماثل، حيث تعتبر هذه التقنية من بين أكثر التقنيات أمانا.

- **تقنية التشفير المتماثل:**

يسمى بتقنية المفاتيح الخصوصية التي تقوم على إستخدام ذات المفتاح الخصوصي أو الرمز في تشفير و فك الشفرة مايعني وجود مفتاح واحد يمتلكه المرسل و المرسل إليه و تصلح هذه التقنية في الأنظمة المغلقة حيث تقوم علاقة بين الأطراف تسهل معرفة هوية المصدر و عملية التأكد من المصدر ويقل إعتماد البنوك على هذه التقنية.

- **تقنية التشفير غير المتماثل:**

هي التقنية الأكثر إستعمالا في المصارف لأنها تؤمن قدرا عاليا من الموثوقية و تسمى يتقنية المفاتيح العمومية التي ترتكز على إستعمال مفتاحين أو رمزين مختلفين الأول خصوصي يعرفه مستخدم معين لشبكة الإنترنيت و يبقى سريا و خاص و الثاني عمومي يحري توزيعه و إبلاغه للجميع الذين يرغبون في تلقي الرسائل من البنك. (مسعودي و مسعودي، 2019، صفحة 436)

- **البصمة الإلكترونية:**

رغم ان التشفير يمنع المتلصصين من الإطلاع على محتويات الرسالة إلا أنه لا يمنع المخربين من العبث بها أي أن التشفير لا يضمن سلامة الرسالة و من هنا ظهرت الحاجة إلى البصمة الإلكترونية للرسالة و هي بصمة رقمية يتم إشتقاقها وفقا لخورزميات معينة تدعى بدوال التمويه إذ تطبق هذه الخوارزميات حسابات رياضية على الرسالة لتوليد بصمة (سلسلة صغيرة) تمثل ملفا كاملا أو رسالة (سلسلة كبيرة) و تدعى البيانات الناتجة بالبصمة الإلكترونية للرسالة. (مسعداوي و سعيدي، 2011، صفحة 08)

- **الجدار الناري:**

عبارة عن مرشحات تتبع صلاحية و حدود الإستخدام للمصرح لهم فقط و إستخدام النظام و على الرغم من أنها تعطل إنتقال البيانات نسبيا إلا أنها ذات فاعلية في منع محاولات الإختراق و التعدي. (بن قارة، 2021، صفحة 32)

تتمثل في أدوات إلكترونية أمنية تمنع الوصول الغير مسموح به إلى الحاسب الشخصي، و ذلك عن طريق إقامة حاجز يفصل بين الشبكة و الحواسيب الشخصية، تجبر به جميع عمليات الدخول و الخروج للمرور عبر هذا الجدار الذي يتصدى لجميع محاولات الدخول بدون صفة. (حمودي، 2020، صفحة 99)

- **التوقيع الإلكتروني:**

عرف قانون الأونسترال للتوقيعات الإلكترونية لعام 2001 التوقيع الإلكتروني على أنه : "بيانات في شكل إلكتروني مدرجة في رسالة بيانات أو مضافة إليها، أو مرتبطة بها منطقيا، يجوز أن تستخدم لتعيين هوية الموقع على المعلومات الواردة في رسالة البيانات".

فلقد ركز هذا القانون على مسألتين أساسيتين هما: تعيين هوية الشخص الموقع، و موافقته على المعلومات الواردة في المحرر، و ينجر عن التوقيع الإلكتروني جريمة الإعتداء على النظام المعلوماتي للتوقيع الإلكتروني، و الذي يتحقق من خلال الإعتداء على النظام المعلوماتي له، وهذا بالدخول أو البقاء غير المصرح لهما. (حمودي، 2020، صفحة 99)

- **برتوكولات الحركات المالية الآمنةSET:**

الغاية من هذا البروتوكول ضمان الحفاظ على أمن البيانات (خصوصيتها و سلامتها و التحقق من وصولها إلى الجهة المطلوبة) أثناء إجراء الحركات المالية عبر شبكة مفتوحة مثل الإنترنيت، يستخدم هذا البروتوكول برمجيات تدعى برمجيات المحفظة الإلكترونية و هي تحتوي على رقم حامل البطاقة و الشهادة الرقمية التابعة له، أما التاجر فتكون له شهادة رقمية صادرة عن أحد البنوك المعتمدة و يستخدم كل من حامل البطاقة و التاجر الشهادة الرقمية التابعة له مما يتيح لكل منهما التحقق من هوية الآخر عند إجراء الحركات المالية عبر الإنترنيت و لا يمكن للتاجر مشاهدة رقم البطاقة الإئتمانية أثناء جلسة برتوكول الحركات المالية الآمنة حيث ترسل الصيغة المشفرة لهذا الرقم إلى مصدر هذه البطاقة للموافقة على إجراء الحركة المالية مع التاجر و تضمن هذه الطريقة عدم عرض الرقم كما تمنع أي تعديل غير مرخص به أثناء إرسال البيانات.

- **برتوكولات الطبقات الأمنية SSL:**

هو برنامج به بروتوكول تشفير متخصص لنقل البيانات و المعلومات المشفرة بين جهازين عبر شبكة الإنترنيت بطريقة آمنة بحيث لا يمكن أي شخص قراءتها غير المرسل و المستقبل و في نفس الوقت تكون قوة التشفير فيها قوية و يصعب فكها و يقوم هذا البرنامج بربط المتصفح الموجود على حاسوب

المستخدم (المشتري=المستهلك) بالحاسوب المزود(الخادم) الخاص بالموقع المراد الشراء منه و هذا طبعا إذا كان حاسوب الخادم مزود بهذه التقنية و يقوم هذا البرنامج بتشفير أي معلومة صادرة من ذلك المتصفح وصولا إلى حاسوب الخادم الخاص بالموقع بإستخدام بروتوكول التحكم بالإرسال و بروتوكول الإنترنيت الذي يعرف بـ ip / tcp و لقد سميت بالطبقة الآمنة لأن هذا البرنامج يعمل كطبقة وسطية تربط بين بروتوكول التحكم بالنقل. (مسعداوي و سعيدي، 2011، صفحة 09)

لم تسلم أنظمة الدفع الإلكترونية من الجرائم المعلوماتية و هذا راجع للتطورات التكنولوجية و الرقمنة، لذا أصبح من الضروري تبني الأمن المعلوماتي لمساهمته في تحقيق السرية و الأمان لمختلف المعاملات و المعلومات الإلكترونية بإعتباره الضمانة الأساسية لنجاح الصيرفة الإلكترونية و كلما كان الأمن المعلوماتي متوفر كلما كانت الصيرفة الإلكترونية أكثر فعالية.

4. تجربة الجزائر في مجال أمن المعلومات المصرفية

قصد تحقيق الأمن في المعاملات المالية الإلكترونية في الجزائر تم إبرام إتفاقية شراكة في جانفي 2004 مابين المجموعة الفرنسية riagram-edi الرائدة في مجال البرمجيات المتعلقة بالصيرفة الإلكترونية وأمن تبادل البيانات المالية و ثلاثة مؤسسات جزائرية المتمثلة في: (cerist, engineering, multimedia magact soft) لتنشأ شركة مختلطة سميت بالجزائر لخدمات الصيرفة الإلكترونية و تقدم هذه الشركة خدمات متعلقة بالبنوك عن بعد و تسيير و أمن تبادل البيانات المالية لجميع البنوك حيث ساهمت هذه الشركة في بناء مواقع إلكترونية بصيغة المصرف الإلكتروني على غرار البنك الخارجي الجزائري و القرض الشعبي الجزائري.. إلخ لعصرنة الخدمات المصرفية و أنظمة الدفع الإلكترونية، و أنشئت هذه الشركة من أجل هدف أساسي هو تلبية حاجيات المؤسسات المالية بإقتراح برمجيات تقدم خدمات عن طريق برمجيات متعددة و من أهم خدماتها.

- إقتراح حلول إدارة الخزينة، البنوك عن بعد و إستخدام النقد الإلكتروني؛
- تبسيط و تأمين المبادلات الإلكترونية و تزويد زبائنها بكل تطور تكنولوجي جديد؛
- تقديم خدماتها يكون بصفة مستمرة طوال مدة الإستفادة منها.

إن إستراتيجية أمن المعلومات المصرفية و حمايتها في بيئة الإنترنيت تستوجب على المصارف الجزائرية إتخاذ إجراءات مشددة من الحيطة و الحذر و المراقبة لرفع مستوى الحماية للخدمات المصرفية الإلكترونية التي تقدمها و الإلتزام التام بالضوابط الأمنية المحددة للأنظمة الإلكترونية المصرفية، فإهتمام المصارف الجزائرية بقضية الأمن المعلوماتي يوفر ثقة العملاء في الخدمات الإلكترونية التي تنتهجها. (زيدان و حمو، 2015، صفحة 177)

1.4 النصوص القانونية الجزائرية التي أشارت إلى الأمن المعلوماتي لنظم الدفع الإلكترونية:

جاءت النصوص القانونية المتعلقة بأمن المعلومات مبعثرة بين القوانين المختلفة و أنظمة بنك الجزائر، و في سياق أمن المعلومات الإلكترونية و التي قصد المشرع الجزائري من خلالها الحماية القانونية للمعلومات الإلكترونية.

يعتبر قانون 15/03 المتضمن الموافقة في الأمر 11/03 المتعلق بالنقد و القرض أول قانون جزائري تضمن التعامل الإلكتروني الحديث في القطاع المصرفي و يتضح ذلك من خلال المادة 69 منه التي تنص على أنه:" **تعتبر وسائل الدفع كل الأدوات التي تمكن كل شخص من تحويل أموال مهما يكون السند أو الأسلوب التقني المستعمل**". (كردي، 2017، صفحة 249)

قام المشرع الجزائري بتعديل قانون العقوبات بموجب القانون رقم 04-15 المتضمن الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، المتمم للأمر رقم 66- 156 المتضمن لقانون العقوبات الصادر بتاريخ 10 نوفمبر 2004، حيث جاء في هذا القانون في قسمه السابع مكرر، الذي تضمن ثمانية مواد من المادة 394 إلى المادة 394 مكرر 7، وقد عالجت هذه المواد عدة جوانب متعلقة بتخريب النظام المعلوماتي، الغش في النظام المعلوماتي، إدخال و إزالة و تعديل المعطيات في النظام المعلوماتي.

حيث نصت المادة 394 مكرر فقرة أولى على مايلي: "**يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1)، وبغرامة من 50000 دج إلى 100000 دج كل من يدخل أو يبقى عن طريق الغش في كلّ أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك**". (الجريدة الرسمية للجمهورية الجزائرية، العدد71، صفحة 11)

كما تعتبر أنظمة بنك الجزائر من بين النصوص القانونية التي تناولت مسألة الأمن المعلوماتي حيث صدر سنة 2005 نظام رقم 05-07 مؤرخ في 26 ذي القعدة عام 1426هـ الموافق لـ 28 ديسمبر 2005، المتضمن لأمن أنظمة الدفع، حيث نصت المادة الأولى منه على ما يلي : "**يهدف هذا النظام إلى تعريف أنظمة الدفع و جهاز الأمن الخاص بها**". (الجريدة الرسمية للجمهورية الجزائرية، العدد 37، صفحة 23)

و نصت المادة **الرابعة** فقرة أولى منه على ما يلي :"**يتضمن أمن أنظمة الدفع أمن البنية الأساسية لأنظمة الدفع و كذا أمن وسائل الدفع....**". (الجريدة الرسمية للجمهورية الجزائرية، العدد 37، صفحة 24)

و لقد جاءت الفقرة الثالثة من المادة 4 من النظام السالف الذكر حيث نصت :"**تلقى مسؤولية وضع أجهزة أمن أنظمة الدفع على عاتق مسيريها و المشاركين في هذه الأنظمة، بينما يسهر بنك**

الجزائر على الاشتغال الحسن لهذه الأنظمة و أمنها". (الجريدة الرسمية للجمهورية الجزائرية، العدد 37، صفحة 24)

كما نصت المادة 51 من النظام رقم 05-06 المؤرخ في 13 ذي القعدة عام 1426هـ الموافق لـ 15 ديسمبر سنة 2005 ، يتعلق بمقاصة الصكوك و أدوات الدفع على أنه: **"يجب على المشاركين ان يستعملوا كل حل من شأنه أن يضمن السير الحسن للعمليات، كما يجب عليهم على وجه الخصوص وضع أنظمة النجدة "Back up" من أجل ضمان إستمرارية العمليات".** (الجريدة الرسمية للجمهورية الجزائرية، العدد 26، صفحة 29)

كما نصت على ذلك المادة 60 من النظام 05-04 المؤرخ في 10 رمضان عام 1426هـ الموافق لـ 13 أكتوبر سنة 2005 **يتضمن نظام التسوية الإجمالية الفورية للمبالغ الكبيرة و الدفع المستعجل، حيث أوجبت على المشاركين وضع أنظمة النجدة "Back up"، من أجل ضمان إستمرارية العمليات.** (الجريدة الرسمية للجمهورية الجزائرية، العدد 02، صفحة 34)

كما "**يتكفل بنك الجزائر بالسهر على السير الحسن لأنظمة الدفع و أمنها و يسهر على أمن أنظمة المقاصة و التسوية و تسليم الوسائل المالية**" و ذلك طبقا للمادة 11 من نفس النظام السالف الذكر، و أوجبت المادة 12 من هذا النظام كذلك "**مَهَمة بنك الجزائر في التأكد من أمن بطاقات الدفع و متابعة إجراءات توفير شروط الأمن التي قامت بها الجهات التي تصدرها "البنوك" ، و التجار و متابعة إحصاءات التدليس و التطورات في ميادين التكنولوجيا التي قد تؤثر على أمن بطاقات الدفع".**

كما سن المشرع الجزائري قانونا خاصا بالجريمة الإلكترونية بموجب القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 هـ الموافق لـ 05 أوت2009، المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتهما.

و لقد جاء في فصله الخامس على "**إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحته".** (الجريدة الرسمية للجمهورية الجزائرية، العدد 47، صفحة 08)

و في إطار الأمن المعلوماتي دائما نص نظام بنك الجزائر رقم 12-03 مؤرخ في14 محرم 1434هـ الموافق لـ 28 نوفمبر 2012 ، و المتعلق بالوقاية من تبييض الأموال و تمويل الإرهاب و مكافحتهما في المادة 17 فقرة 2 كما يلي :"**يجب أن يحوز مسيرو نظام الدفع و المتعاملون المباشرون أو غير**

المباشرين على جهاز آلي لإكتشاف الزبائن و العمليات و يتعلق الأمر بالهيئات أو الأشخاص المسجلين في القوائم المعدة مسبقا". (الجريدة الرسمية للجمهورية الجزائرية، العدد 12، صفحة 27)

و لقد أصدر رئيس الجمهورية مرسوم رئاسي رقم 15 -261 مؤرخ في 24 ذي الحجة عام 1436هـ الموافق لـ 8 أكتوبر 2015، حيث يحدد تشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها. حيث نصت المادة الأولى منه على :**أنه تطبيقا لأحكام المادة 13 من القانون 09-04 المؤرخ في 05 أوت2009 ، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها، يهدف هذا المرسوم تحديد تشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و مكافحتها التي تدعى في صلب النص الهيئة.** (الجريدة الرسمية للجمهورية الجزائرية، العدد 53، صفحة 16)

و في إطار القانون رقم 15-04 المؤرخ في 11 ربيع الثاني عام 1436هـ الموافق ل 1 فبراير سنة 2015 الذي يحدد القواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونين السالف الذكر، لم يتضمن مادة صريحة تنص على الأمن المعلوماتي بصريح العبارة، لكن من خلال المادة 30 منه و التي تنص على مهام السلطة الإقتصادية للتصديق الإلكتروني، حيث نصت النقطة 13 منها على "**إجراء كل مراقبة طبقا لسياسة التصديق الإلكتروني، و دفتر الشروط الذي يحدد شروط و كيفيات تأدية خدمات التصديق الإلكتروني".** (الجريدة الرسمية للجمهورية الجزائرية، العدد 60، صفحة 11)

و لقد جاء القانون رقم 18-04 المؤرخ في24 شعبان عام 1439هـ الموافق لـ 10 مايو 2018، و الذي يحدد القواعد العامة المتعلقة بالبريد و الإتصالات الإلكترونية، حيث جاء في المادة 4 منه:" تسهر الدولة في إطار الصلاحيات المرتبطة بمهامها خصوصا على ما يأتي:

- تحديد و تطبيق معايير إنشاء و إستغلال مختلف الخدمات؛
- أمن و سلامة شبكات الإتصالات الإلكترونية؛
- إستمرارية و إنتظام الخدمات المقدمة للجمهور، ...". (الجريدة الرسمية للجمهورية الجزائرية، العدد 27، صفحة 05)

و لقد شهدت سنة 2018 أيضا صدور أول قانون للتجارة الإلكترونية في الجزائر ألا و هو القانون 18-05 المؤرخ في 24 شعبان عام 1439هـ الموافق ل 10 مايو 2018 و الذي حمل في طياته مواد قانونية متعلقة بالتجارة الإلكترونية، في فصله السادس الدفع في المعاملات الإلكترونية، حيث نصت المادة 27 الفقرة 02 على أن الدفع الإلكتروني يتم عبر منصات دفع مخصصة لهذا الغرض، و

لقد نصت المادة 29 من نفس القانون على مايلي :"**تخضع منصات الدفع الإلكتروني المنشأة و المستغلة طبقا للمادة 27 أعلاه، لرقابة بنك الجزائر لضمان إستجابتها لمتطلبات التشغيل البيني و سرية البيانات و سلامتها و أمن تبادلها**". (الجريدة الرسمية للجمهورية الجزائرية، العدد 28، صفحة 08)

5. خاتمة:

تحاول هذه الورقة البحثية الوصول إليه هو تحليل الدور الذي يلعبه الأمن المعلوماتي في حماية أنظمة الدفع الإلكترونية من خلال الربط بين الامن المعلوماتي و الصيرفة الإلكترونية و إبراز العلاقة التكاملية بينهما، حيث كلما كان الامن المعلوماتي متوفر كلما كانت الصيرفة الإلكترونية أكثر فعالية، لماذا لأن الامن المعلوماتي سيضمن السرية و السرعة التي تعتبر من ضمن المبادئ الهامة التي تلتزم بها المصارف في أداء وظائفها و تنمية معاملاتها كما أن الإتجاه نحو المصارف الإلكترونية سيجنب المصارف العادية مشكلة حسن المعاملة التي قد تنتج جراء عدم إحترام موظف ما بالمصرف لأخلاقيات و ضوابط المهنة كون أن المصارف الإلكترونية تتم فيها المعاملة بين الزبون و جهاز الحاسوب المربوط بالموقع المعلوماتي للمصرف، لهذا فإن الأمن المعلوماتي هو الشرط الأساسي لتمتع الخدمة المصرفية الإلكترونية بخصائصها و متطلباتها لاسيما تلك المتعلقة بالسرية و الأمان التي تعتبر شرط أساسي لعامل الثقة الذي يعزز من ولاء الزبائن لمصارفهم.

النتائج:

- تبني الأمن المعلوماتي في المصارف الجزائرية يساهم في تحقيق صيرفة إلكترونية فعالة؛
- الجزائر تشهد تطورا نسبيا قد لا يرقى إلى المستوى المطلوب و لكنه لبنة أساسية تساهم في ترقية العمل المصرفي الإلكتروني؛
- إن إستراتيجية أمن المعلومات المصرفية و حمايتها في بيئة الإنترنيت تستوجب على المصارف الجزائرية إتخاذ إجراءات مشددة من الحيطة و الحذر و المراقبة لرفع مستوى الحماية للخدمات المصرفية الإلكترونية التي تقدمها، حيث توجد بيئة قانونية بشان أمن نظم الدفع إلا أنها غير كافية في مواجهة الجرائم الإلكترونية.

التوصيات:

- أهمية حصول المصارف الجزائرية على أحدث التقنيات الحديثة سواء فيما يتعلق بالأجهزة أو البرامج لمواجهة أحدث التطورات و الأساليب المتبعة في مجال الهجمات و القرصنة

الإلكترونية الدولية، بهدف إقتناء جدار أمني أكثر فعالية و قادر على التصدي لأحدث الأساليب المتبعة في هذا الشأن؛

- سن القوانين الأمنية و إلزام المصارف بتطبيقها و معاقبة مخالفيها والتي من شأنها ان تعمل على تعزيز الإجراءات الأمنية و كشف الفجوات الأمنية؛
- الإستفادة من خبرات المصارف العالمية في مجال الأمن المعلوماتي و مواجهة القرصنة؛
- أهمية إستحداث تخصص الأمن المعلوماتي في الجامعات الجزائرية المتخصصة في مجال تقنية المعلومات إقتداءا بالجامعات العالمية، بهدف خلق الكوادر العربية المتخصصة ذات المستوى العالي في هذا المجال؛
- إلزام المصارف الجزائرية بإجراء إختبارات الضغط (stress testing) لتحديد حجم الأثار المترتبة على نجاح أية عمليات قرصنة تتعرض لها أنظمتها الإلكترونية.

المراجع:

- الجريدة الرسمية للجمهورية الجزائرية. (العدد 02). 15 ذو الحجة 1426هـ الموافق ل 15 يناير سنة 2006م.
- الجريدة الرسمية للجمهورية الجزائرية. (العدد 12). 16 ربيع الثاني 1434هـ الموافق ل 27 فبراير سنة 2013م .
- الجريدة الرسمية للجمهورية الجزائرية. (العدد 26). 24 ربيع الاول 1427هـ الموافق ل 23 اريل سنة 2006م.
- الجريدة الرسمية للجمهورية الجزائرية. (العدد 27). 27 شعبان 1439هـ الموافق ل 13 مايو سنة 2018م.
- الجريدة الرسمية للجمهورية الجزائرية. (العدد 28). 30 شعبان 1439هـ الموافق ل 16 مايو سنة 2018م .
- الجريدة الرسمية للجمهورية الجزائرية. (العدد 37). 08 جمادى اولى 1427هـ الموافق ل 04 يونيو سنة 2006م.
- الجريدة الرسمية للجمهورية الجزائرية. (العدد 47). 25 شعبان 1430هـ الموافق ل 16 غشت سنة 2009م.
- الجريدة الرسمية للجمهورية الجزائرية. (العدد 53). 24 ذي الحجة 1436هـ الموافق ل 08 اكتوبر سنة 2015م .

- الجريدة الرسمية للجمهورية الجزائرية. (العدد 60). 20 ربيع الثاني 1436هـ الموافق ل 10 فبراير سنة 2015م .
- الجريدة الرسمية للجمهورية الجزائرية. (العدد71). 27 رمضلن 1425هـ الموافق ل 10نوفمبر سنة 2004 م.
- امن المعلومات في القطاع المصرفي المخاطر و التحديات. (04 ابريل, 2018). سياتيك. تاريخ الاسترداد 29 12, 2021، من سياتيك: https://www.ciatec.com
- حسين علي قاسم الشمالي. (2017). امن و سرية المعلومات و اثرها في الأداء المصرفي: دراسة تطبيقية على البتوك العاملة في الأردن. مجلة جامعة القدس المفتوحة للابحاث و الدراسات الادارية و الاقتصادية، 02(04).
- رشيد بوعافية، و محمد صالح زويتة. (2010). الصيرفة الالكترونية-الواقع و التحديات-. مجلة الاقتصاد الجديد، 01(02).
- رشيدة اكسوم عيلام. (2018). المركز القانوني للمستهلك الالكتروني. اطروحة الدكتوراه في القانون . كلية الحقوق و العلوم السياسية، تيزي وزو: جامعة مولود معمري.
- سلمان بن علي بن وهف القحطاني. (2003). امن المعلومات في ضوء التطور التقني و التكنولوجي الحديث في الشبكات اللاسلكية النقالة. المؤتمر العلمي الأول حول الجوانب القانونية و الأمنية للعمليات الالكترونية. اكاديمية شرطة دبي، مركز البحوث و الدراسات، دبي –الامارات العربية المتحدة. تاريخ الاسترداد 26-28 افريل, 2003
- عائشة مصطفى بن قارة. (2021). استراتيجية تحقيق الامن المعلوماتي للحكومة الالكترونية في الجزائر. المؤتمر الدولي الشامل للقضايا النظرية و سبل معالجتها العملية. 02. دار رافد للنشر.
- عبد الهادي مسعودي ، و خيرة مسعودي. (2019). محددات و متطلبات حماية الانظمة المعلوماتية في المصرف. مجلة الاقتصاد الجديد، 10(01).
- عدمان مريزق، و عماد بوقلاشي. (2010). الامن المعلوماتي في ظل التجارة الالكترونية-اشارة الى حالتي تونس و الجزائر-. مجلة الاقتصاد الجديد، 01(02).
- فريدة حمودي. (2020). الامن المعلوماتي في الجزائر بين التطورات التكنولوجية و ضعف البيئة الرقمية المجال المصرفي نموذجا "دراسة قانونية". مجلة جيل الابحاث القانونية المعمقة(41).
- محاد عريوة، و محمد خاوي. (2017). واقع وسائل و أنظمة الدفع الالكترونية في النظام البنكي الجزائري. مجلة الدراسات الاقتصادية المعاصرة، 02(04).

- ملاك قارة. (2016). الجريمة المعلوماتية في القطاع البنكي و أساليب مكافحتها إشارة لحالة الجزائر. مجلة جامعة الامير عبد القادر للعلوم الاسلامية، 30(04).
- نبيلة كردي. (2017). الشيك الالكتروني. مجلة العلوم الاجتماعية و الانسانية، 10(02).
- نور الدين بربار، و محمد هشام قلمين. (2014). دور الامن المعلوماتي في تفعيل نشاط الصيرفة الالكترونية. مجلة الاقتصاد و التنمية، 02(01).
- يوسف مسعداوي، و جميلة سعيدي. (2011). وسائل الدفع الالكترونية. الملتقى الدولي الرابع: عصرنة نظام الدفع في البنوك الجزائرية و اشكالية اعتماد التجارة الالكترونية في الجزائر-عرض تجارب دولية-. المركز الجامعي خميس مليانة. تاريخ الاسترداد 26-27 افريل, 2011