Journal of Economic Growth and Entrepreneurship JEGE
Spatial and entrepreneurial development studies laboratory
Year : 2020 Vol.4 No.1 pp:67-74.

Mechanisms of managing electronic banking risks in the Algerian banking system

Djelaila Abdeldjalil[1], Ouafi Nadjem[2],

[1]Doctor, Economic, University AHMED Draia Adrar, Algeria, abd.djelaila@univ-adrar.dz
[2]D octor, Economic, University AHMED Draia Adrar, Algeria, abd.djelaila@univ-adrar.dz

ARTICLE INFO

Article history:
Received: 02/02/2020
Accepted: 01/05/2020
Online: 02/05/2020

Keywords:
Electronic banking
Banking risks
Risk Management
Basel document
JEL Code: E59,O14

ABSTRACT

E-banking is a prerequisite in the equation of any banking industry in the world, due to the multiple benefits that it has for the bank and the customer alike, however, with the growth of these electronic banking businesses, the need to manage and monitor their risks has emerged, in order to reduce and control those risks. In order to reconcile achieving the goals of banks on the one hand, and to meet the desires and aspirations of customers on the other hand. This research paper aims to introduce the management of risks related to electronic banking in its international garment, as it seeks to uncover the state of the Algerian banking system and the extent of its conformity with international standards emanating from the Basel Committee, and the study found the weakness of Algerian legislation in this field, with a slow pace with global standards, as recommended With a set of recommendations, such as the need to activate banking supervision of electronic banking, and to benefit from the experiences of some Arab countries

آليات إدارة مخاطر الصيرفة الإلكترونية في المنظومة المصرفية الجزائرية

جلايلة عبد الجليل[1]، وافي ناجم[2]

[1] دكتور، اقتصاد، جامعة أحمد دراية أدرار، الجزائر، abd.djelaila@univ-adrar.dz
[2] دكتور، اقتصاد، جامعة أحمد دراية أدرار، الجزائر، oua.nadjem@univ-adrar.dz

معلومات المقال

تاريخ الاستقبال:
2020/02/02:
تاريخ القبول: 2020/05/01
تاريخ النشر: 2020/05/02

الكلمات المفتاحية
الصيرفة الإلكترونية
مخاطر مصرفية
إدارة المخاطر
وثيقة بازل
JEL Code: E59,O14

الملخص

تعتبر الصيرفة الإلكترونية متطلب اساس في معادلة اي صناعة مصرفية في العالم، وذلك لما توفره من مزايا متعددة للبنك والعميل على حد سواء، إلا أنه مع تنامي هذه الأعمال المصرفية الإلكترونية، ظهرت الحاجة إلى إدارة مخاطرها ومراقبتها، وذلك للحد من تلك المخاطر، والتحكم فيها بغية التوفيق بين تحقيق أهداف البنوك من جهة، وتلبية لرغبات وتطلعات الزبائن من جهة أخرى.

تهدف هذه الورقة البحثية إلى التعريف بإدارة المخاطر المتعلقة بالصيرفة الإلكترونية في ثوبها الدولي، كما أنها تسعى الى كشف حال المنظومة المصرفية الجزائرية ومدى مواكبتها للمعايير الدولية المنبثقة عن لجنة بازل، وتوصلت الدراسة إلى ضعف التشريع الجزائري في هذا المجال، بمسايرة بطيئة للمعايير العالمية، كما أوصت بجملة من التوصيات، كضرورة تفعيل الرقابة المصرفية على الصيرفة الإلكترونية، والاستفادة من خبرات بعض الدول العربية.

- مقدمة:

* *DJELAILA ABDELJALIL, abd.djelaila@univ-adrar.dz:*

تهتم كل الصناعات المصرفية بمنتجات الصيرفة الإلكترونية، ذلك أنها تعتبر القاسم المشترك بين العمل المصرفي التقليدي ومفرزات التكنولوجيا الحديثة، خاصة في مجال الاتصال، ومن خلال هذا النوع من الصيرفة تم سد بعض النقائص المرتبطة بالصيرفة التقليدية، خاصة فيما يخص تجاوز عنصري الزمن والمكان، فأضحت الخدمات المصرفية الإلكترونية تقدم في أي وقت وفي أي مكان، وبالتالي تلبية متطلبات الزبائن في أوقات مختلفة، وأمكنة متعددة، إلا أنه صاحبت هذه الطفرة من العمل المصرفي مخاطر مصرفية، هددت الكيانات المصرفية المقدمة لهذه المنجات المصرفية، وبات من الضروري إدارة مخاطر الصيرفة الإلكترونية، بشكل سليم يحد من تلك المخاطر ويساعد على تحقيق أهداف البنوك المحددة مسبقاً، ولقد كان للجنة بازل دوراً مهماً في هذا الصدد، باصدارها لوثيقتين الأولى شهر ماي 2001، والثانية شهر جويلية 2003، حيث تعد وثيقة بازل لإدارة مخاطر الصيرفة الإلكترونية، القالب الدولي للرقابة المصرفية على الصيرفة الإلكترونية، وإدارة مخاطرها، وصمام الأمان الموجه لعمل مصرفي إلكتروني سليم.

وتقدم البنوك التجارية الجزائرية مصفوفة من الخدمات المصرفية الإلكترونية، مثل نظام ATCI ونظام ARTS، وخدمات البطاقات البنكية، لكن السؤال المطروح والذي يعتبر محور إشكالية الدراسة، إلى أي مدى تتوافق المنظومة المصرفية الجزائرية مع المعايير الدولية لإدارة مخاطر الصيرفة الإلكترونية؟

وتكمن أهمية الدراسة في تسليط الضوء على أهم التنظيمات الصادرة من قبل بنك الجزائر بصفته البنك المركزي، التي تنظم العمل المصرفي الإلكتروني في الجزائر، خاصة مع التوجه الملحوظ للجزائر نحو الصيرفة الإلكترونية منذ سنة 2005، وذلك بصدور النظام 05-04 المتعلق بنظام ARTS، والنظام 05-06 المتعلق بنظام ATCI، وحتى قانون المالية التكميلي 2020 ألزم التجار بضرورة توفير أجهزة الدفع الإلكترونية (TPE) مع نهاية السنة، هذه المعطيات والحاجة الملحة لتبني الصيرفة الإلكترونية في الجزائر، يجعل من الإطار الرقابي للنشاط المصرفي الإلكتروني في الجزائر وإدارة مخاطره ذو أهمية بالغة للدراسة، وبالتالي تهدف هذه الأخيرة إلى المقاربة بين الاطار الدولي للرقابة وإدارة المخاطر المتعلقة بالصيرفة الإلكترونية، والتنظيمات المعمول بها في الجزائر الخاصة بهذا الشأن، والوقوف على مدى مسايرتها لما أصدرته لجنة بازل، كونها تحمل نوع من الإلزام الأدبي الدولي، لما تصدره من مقررات ووثائق، بغية حماية الصناعة المصرفية وسلامتها على المستوى العالمي.

1- إدارة مخاطر الصيرفة الإلكترونية:

1-1- مفهوم إدارة مخاطر الصيرفة الإلكترونية:

إن تكثيف أنشطة البنوك قد يكون سبباً استراتيجياً للانخراط في الأنشطة المصرفية الإلكترونية فينعكس إيجاباً على كفاءة البنك، وبالنفع على الزبائن والتجار، وفي الوقت نفسه تزيد المخاطر المصرفية للبنوك المشاركة في الأنشطة المصرفية الإلكترونية، وعلى اثر ذلك يتوجب على البنوك، إعداد موازنة بين المخاطر والعوائد، بحيث تكون البنوك قادرة على إدارة المخاطر والسيطرة عليها واستيعاب أي خسائر ذات صلة إذا لزم الأمر، ومن المرجح أن تؤدي الوتيرة السريعة للابتكار التكنولوجي إلى تغير طبيعة ونطاق المخاطر التي تواجهها البنوك المقدمة لخدمات مصرفية إلكترونية، ويتوقع المشرفون على الصناعة المصرفية أن تكون للبنوك عمليات تمكنها من الاستجابة للمخاطر الحالية، والتكيف مع المخاطر الجديدة بحيث تشمل عملية إدارة المخاطر على ثلاثة عناصر أساسية، تقييم المخاطر والسيطرة على التعرض للمخاطر، ومراقبة المخاطر، وتستخدم هذه العناصر الثلاثة لعملية إدارة المخاطر المصرفية بصورة خاصة من طرف البنوك الناشطة في المجال المصرفي الإلكتروني (SOLANKI, september2012).

وترتكز الصناعة المصرفية على عملية إدارة المخاطر، خاصة ما تعلق بالصيرفة الإلكترونية لما يحيطها من مخاطر، نظراً لطبيعتها المستمدة من التطورات التكنولوجية، التي تتطلب مسايرة ومواكبة لكل هذه التغيرات والمستجدات التي من شأنها التأثير المباشر على العمل المصرفي الإلكتروني، وبالتالي تعمل البنوك من خلال إدارة المخاطر على وضع إجراءات وقائية وتصحيحية، تحد بواسطتها أي خطر يؤدي إلى انحراف أهداف البنك عن المسار المرسوم والمخطط له مسبقاً لتحقيق ذلك.

2.1- مبادئ إدارة المخاطر المصرفية الإلكترونية:

تشمل إدارة المخاطر المصرفية الإلكترونية على كل من التقييم والرقابة والمتابعة، وذلك وفق مايلي (وسيم محمد الحداد، 2012):

أ- تقييم المخاطر Assessing risks:

إن عملية تقييم المخاطر تنقسم إلى خطوتين وهما:

- تحديد المخاطر المصرفية التي تتعرض للبنك، وتحديد ما مدى تأثيرها عليه؛
- وضع حدود قصوى لما يمكن للبنك أن يتحمله من خسائر، جراء التعامل مع هذه المخاطر، أي تسقيف مستوى التعرض لها بما يسمح للبنك من تحقيق أهدافه؛

ب- الرقابة على التعرض للمخاطر risk exposuves Controlling :

تشتمل عملية الرقابة عن التعرض للمخاطر، على التحقق من مدى الانضباط في تنفيذ سياسات وإجراءات التأمين من قبل البنك، وكذلك إعداد خطط طوارئ بديلة في حالة إخفاق النظم عن أداء الخدمات، ثم متابعة المخاطر عن طريق اختبار النظم وإجراء المراجعة الداخلية والخارجية؛

3.1- مراحل إدارة مخاطر الصيرفة الإلكترونية:

تمر عملية إدارة مخاطر الصيرفة الإلكترونية عبر مراحل مختلفة، حيث أنها متكاملة تؤدي إلى الحد من تلك المخاطر أو التقليل من آثارها إلى حد أدنى، نذكرها كالآتي (بن عيدة، 2018):

أ- تحديد المخاطر: يتم تحديد المخاطر التي تحيط أو تتعرض لكل منتج أو خدمة مصرفية، فعملية تحديد المخاطر تعتبر أساس إدارة المخاطر المصرفية، ويجب أن تكون هذه الخطوة مستمرة ومتواصلة؛

ب-قياس المخاطر: تأتي هذه الخطوة مباشرة بعد عملية تحديد المخاطر، بحيث يجب النظر لكل خطر بأبعاده الثلاثة، حجمه، مدته واحتمالية حدوثه، وتُعني إدارة المخاطر للوقت الذي تتم فيه عملية قياس المخاطر أهمية بالغة؛

ج- ضبط المخاطر: يطلق على الخطوة الثالثة من عملية إدارة المخاطر المصرفية الإلكترونية، ضبط المخاطر، وتكون عملية الضبط من خلال ثلاثة أساليب، الأسلوب الأول بجنب بعض النشاطات المؤدية إلى التعرض إلى مخاطر مصرفية، الأسلوب الثاني تقليل أثر المخاطر المصرفية، أما الأسلوب الثالث فيتمثل في إلغاء أثر المخاطر المصرفية تماما؛

د- مراقبة المخاطر: عنلى البنوك أن تسعى إلى إيجاد نظام معلومات ذو قدرة على تحديد قياس المخاطر المصرفية بدقة، ويسمح بمراقبة التغيرات والمخاطر المرافقة لها.

4.1- إدارة مخاطر الصيرفة الإلكترونية وفق لجنة بازل:

تنقسم مبادئ إدارة مخاطر الصيرفة الإلكترونية المعتمدة في تقرير لجنة بازل الصادر في شهر جويلية 2003م إلى ثلاث فئات عريضة، وغالباً ما تكون متداخلة، ومع ذلك لا يتم تصنيف هذه المبادئ حسب ترتيب الأفضلية أو الأهمية، فإذا كان هذا الترجيح قد يتغير مع مرور الوقت، فمن الأفضل إلتزام الحيادية في الترتيب، وتجنب الأولويات في ذلك، وهي (Basel Committe, july 2003) كالآتي:

أ-مجلس الإدارة والرقابة (المبادئ من 1 إلى3):

المبدأ 1: تفعيل رقابة إدارية فعالة على أنشطة الصيرفة الإلكترونية؛

المبدأ 2: إنشاء عملية مراقبة آمنة شاملة؛

المبدأ 3: وجوب الاهتمام وعملية الرقابة الإدارية الشاملة للعلاقات مع المجهزين الخارجين والأطراف الأخرى؛

ب-ضوابط الأمن (المبادئ من 4إلى10):

المبدأ 4: التحقق من هوية عملاء الخدمات المصرفية الإلكترونية.

المبدأ 5: عدم الرفض والمساءلة عن المعاملات المصرفية الإلكترونية؛

المبدأ 6: أخذ التدابير المناسبة لضمان الفصل بين الواجبات، وذلك من خلال إرساء ضوابط مناسبة للتخويل وصلاحيات الولوج إلى النظم المصرفية الإلكترونية إلى قواعد البيانات؛

المبدأ 7: تحديد ضوابط ترخيص سلمية داخل الأنظمة المصرفية الإلكترونية وقواعد البيانات والتطبيقات؛

المبدأ 8: ضمان سلامة بيانات المعاملات المصرفية الإلكترونية، والسجلات والمعلومات؛

المبدأ 9: إنشاء مسارات تدقيق واضحة للمعاملات المصرفية الإلكترونية؛

المبدأ 10: سرية المعلومات المصرفية الأساسية؛

ج-إدارة المخاطر القانونية والسمعة (المبادئ من 11-14):

المبدأ 11: الإفصاحات المناسبة للخدمات المصرفية الإلكترونية؛

المبدأ 12: خصوصية معلومات العميل؛

المبدأ 13: قدرة واستمرارية العمل والتخطيط للطوارئ لضمان توافر الأنظمة والخدمات المصرفية الإلكترونية؛

المبدأ 14: التخطيط للاستجابة إلى الحوادث.

إضافة إلى هذا فلقد جاءت نفس الوثيقة الصادرة عن لجنة بازل سنة 2003م، الممارسات الواجب مراعاتها في إدارة مخاطر الصيرفة الإلكترونية وذلك من خلال ستة ملاحق هي (Basel Committe, july 2003, p. 22) كالتالي:

الملحق الأول: الممارسات السليمة لرقابة أمان العمليات المصرفية الإلكترونية؛

الملحق الثاني: الممارسات السليمة لإدارة الأنظمة والخدمات المصرفية الإلكترونية الخارجية؛

الملحق الثالث: ممارسة الترخيص السليمة لتطبيقات العمليات المصرفية الإلكترونية؛

الملحق الرابع: الممارسات السليمة لمراجعة الحسابات للأنظمة المراقبة الإلكترونية؛

الملحق الخامس: الممارسات السليمة للمساعدة في الحفاظ على خصوصية معلومات عملاء الصيرفة الإلكترونية؛

الملحق السادس: الممارسات السليمة الخاصة بتخطيط الطاقة واستمرارية النشاط والطوارئ؛

ولقد جاءت لجنة بازل بمعاييرها الدولية للحد من مخاطر العمل المصرفي الإلكتروني ولضمان السرية والأمان في تنفيذ عمليات الدفع الإلكترونية، وألزمت جميع البنوك من خلال مقررات بازلII من إدراج المخاطر التشغيلية ضمن المخاطر المصرفية، وانطوت المخاطر الناجمة من أنظمة الدفع المصرفي الإلكتروني تحت تلك المخاطر التشغيلية، كما هو الأمر في تقرير اللجنة شهر جويلية 2003، واعتبرت فيه أن البنك ملزم بتأمين جميع وسائل الأمان والحماية للوسائط الإلكترونية التي يعتمدها، والمعلومات التي يتداولها ومن بين هذه الممارسات نذكر (محمد طاهر، 2015) مايلي:

- ✓اتخاذ التدابير اللازمة للتأكد من هوية صلاحيات الزبائن؛
- ✓أن يعتمد البنك عن طريقة مثالية للتأكد من صحة وسلامة العمليات المصرفية الإلكترونية؛
- ✓استخدام الوسائل الكفيلة بحماية أنظمة الدفع الإلكتروني، وحساب العملاء ومعلوماتهم؛
- ✓اعتماد طرق رقابية مناسبة على الأنظمة الإلكترونية، وكذا صلاحيات الولوج إلى النظام المعلوماتي والبيانات والبرامج التطبيقية؛
- ✓اتخاذ مجموعة من التدابير للحفاظ على سرية المعلومات والبيانات المصرفية ومن بين هذه التدابير مايلي:

- منح الدخول إلى المعلومات والبيانات الشخصية للعميل وحساباته، إلا للأشخاص والجهات الموكول لها لقيام بذلك وبشكل محدود؛

- حماية المعلومات من الإطلاع غير المسموح عليها أو تعديلها، وذلك من خلال نقلها عبر الوسائط الإلكترونية للاتصالات؛
- حماية المعلومات من أطراف أخرى متعاقدة مع البنك لأداء بعض المهام المطلوبة من طرف بنك العميل؛
- مراجعة جميع العمليات المصرفية الإلكترونية، والمعلومات المتعلقة بها وذلك للتأكد من سلامتها، وأن إجراءها تم من طرف أشخاص مرخص لهم بذلك.

من خلال ما سبق ذكره يمكن القول أن محيط العمل المصرفي الإلكتروني مليء بمخاطر مصرفية متعددة، وذلك نظراً لحدة المنافسة بين البنوك في هذا المجال، خاصة ما تعلق بالتسابق لتبني منتجات مصرفية حديثة، وكذلك الطبيعة غير مستقرة للتكنولوجيا التي تتحسن وتطور بوتيرة متسارعة، إضافة إلى هذا الرأس المال البشري الذي يحتاج إلى تدريب مستمر وخبرة لتقديم هذه الخدمات المصرفية الإلكترونية، والتي تعتمد فيها البنوك على أطراف خارجية من خلال التعاقد مع مقدمي خدمات آخرين، زد إلى كل هذا إمكانية حدوث عمليات الاحتيال المالي المعلوماتي، والجرائم الإلكترونية التي تسبب في إتلاف النظم والبيانات الخاصة بالبنك، ولهذه الأسباب وغيرها، كان من الضروري الاهتمام بعملية إدارة المخاطر المصرفية الإلكترونية وكانت في ثوبها الدولي بصدور تقرير لجنة بازل في شكل وثيقة صدرت شهر ماي 2001م، وعدلت هذه الأخيرة بوثيقة أخرى صدرت جويلية 2003م، بموجبها ألزمت العمل المصرفي الإلكتروني، في صورة البنوك المقدمة لهذه الخدمات، بتفعيل عملية الرقابة عن أنشطة الصيرفة الإلكترونية بصورة شاملة على كل المتدخلين في تقديم خدماتها، بما في ذلك الأطراف الخارجية المتعاقدة مع البنك في تقديمها، كما يتوجب على البنوك أيضاً الأخذ بالتدابير الأمنية المناسبة والسليمة لحماية النظم والبيانات المعلوماتية، ولضمان سلامة العمليات المصرفية والمعلومات الخاصة بالعميل، والحفاظ على السرية في معالجة العمليات طوال فترة تنفيذها، ولاستمرارية هذا النوع من الصناعة المصرفية، أجبرت لجنة بازل البنوك على وضع خطط للطوارئ بهدف الاستجابة إلى أي حادث.

2. إدارة المخاطر المصرفية الإلكترونية من خلال الضوابط الرقابية المصرفية على الصيرفة الإلكترونية الواردة في تشريعات بنك الجزائر:

ما يلفت الانتباه عند تسليط الضوء على إدارة المخاطر المصرفية الإلكترونية في الجزائر، وذلك من خلال دراسة الضوابط الرقابية للصيرفة الإلكترونية في المنظومة المصرفية الجزائرية، هي تلك المواد المتفرقة داخل التنظيمات الخاصة بالرقابة المصرفية عامة، أو التنظيمية الخاصة بوسائل الدفع الإلكترونية، والتي يقوم بنك الجزائر عبرها بتنظيم وضبط العمليات المصرفية الإلكترونية، باستثناء ذلك النظام الذي تناول بشكل صريح وحصري أمن أنظمة الدفع سنة 2005م، وبهذا يغيب عن المنظومة المصرفية الجزائرية تشريع مكتمل ومخصص للعمليات المصرفية الإلكترونية أو البنوك الإلكترونية، وذلك إذا ما قمنا بمقارنة بسيطة مع بعض الدول العربية، فعلى سبيل المثال لا الحصر نجد أن مصر وضعت إطاراً عاماً لحوكمة أنظمة المعلومات بالقطاع المصرفي، وإدارة المخاطر المرتبطة بتقديم الخدمات المصرفية عبر القنوات الإلكترونية وذلك بإصدار البنك المركزي المصري القواعد المنظمة لتقديم الخدمات المصرفية عبر الانترنت في القطاع المصرفي المصري بتاريخ 9 نوفمبر 2014م، بحيث شمل هذا التشريع العديد من الجوانب المنظمة للعمل المصرفي الإلكتروني وإدارة المخاطر المرافقة له، كما حمل في طياته أيضاً اعتبارات أمن العملاء وضوابط وقائية خاصة برسائل البريد الإلكتروني والمواقع الإلكترونية، وكذلك الأمر نفسه بالنسبة للكويت بإصدارها مجموعة من التعليمات المنظمة لأعمال الدفع الإلكتروني للأموال، عبر تعميم رقم (2/ر ب، ر ب أ /2018/415) المؤرخ في 23 سبتمبر 2018م، حيث تناول عدة من المحاور تخص تعليمات تنظيم أعمال الدفع الإلكتروني للأموال، وتنظيم النشاط، تنفيذ خدمات النشاط وسرية المعلومات، حدود التعامل اليومية وتغطية المخاطر، وسائل الدفع والإشراف والرقابة، والقيود والجزاءات، وبهذين المثالين يمكن القول أن البنوك المركزية لكل من مصر والكويت أعطت أهمية للرقابة على الصرفية الإلكترونية وإدارة مخاطرها، بتخصيص مجموعة من الضوابط لهذه العمليات المصرفية، عكس ما هو عليه الحال في الجزائر، ذلك أن بنك الجزائر يفتقد لتشريع خاص وواضح يضبط هذا

النوع من الصناعة المصرفية، وربما يرجع ذلك لعدة اعتبارات، منها محدودية انتشار المعاملات الفردية المسواة عن طريق الصيرفة الإلكترونية، وشبه غياب تام للتجارة الإلكترونية.

1.2- النظام 02-03 المتضمن المراقبة الداخلية للبنوك والمؤسسات المالية:

يعد النظام رقم 02-03 المؤرخ في 14 نوفمبر 2002م، المتضمن المراقبة الداخلية للبنوك والمؤسسات المالية بمثابة اللبنة الأساسية لمفهوم الرقابة الداخلية على البنوك والمؤسسات المالية في الجزائر، حيث يهدف هذا النظام إلى تحديد مضمون تلك الرقابة الداخلية، والتي يتوجب على البنوك والمؤسسات المالية إقامتها، وبالأخص الأنظمة المتعلقة بتقدير وتحليل المخاطر، والأنظمة الخاصة بمراقبتها والتحكم فيها، ولقد عرفت المادة الثانية من هذا النظام الخطر العملياتي، بأنه أي خطر ناجم عن نقائص تتخلل إجراءات القيد في النظام المحاسبي، المتعلقة عموماً بأنظمة الإعلام الخاصة بمجموعة الأحداث المترتبة عن عمليات البنك أو المؤسسة المالية المعنية، وبهذا يمكن ربط هذا الخطر بالعمليات المصرفية الإلكترونية التي تلعب فيها نظم الإعلام دوراً مهماً في تنفيذها، تقييدها وتخزينها.

ولقد نصت المادة 18 من نفس النظام على البنوك والمؤسسات المالية، أن تجدد مستوى الأمن الذي تراه ضرورياً في ميدان المعلوماتية، بشكل يتوافق مع متطلبات نشاطاتها، بحيث يجب أن تتأكد من استمرارية استجابة أنظمة المعلومات الخاصة بها إلى هذا الحد الأدنى من الأمن المعتمد (النظام 02-03، 2002). وبهذا نلاحظ أن الجزائر سايرت في هذا الجانب تقرير لجنة بازل الخاص بإدارة المخاطر الرئيسية للصرفة الإلكترونية الصادر في شكل وثيقة شهر ماي 2001م، وذلك في المبدأ 13 من المحور الثالث للمبادئ الرئيسية لإدارة مخاطر الصيرفة الإلكترونية.

أما المادة 19 من النظام 02-03 فلقد أوضحت أهداف مراقبة أنظمة الإعلام الآلي ولخصتها في التأكد بصفة دورية من التقويم لمستوى أمن أنظمة الإعلام، ومن إجراءات التصحيحات الخاصة بهذه الأنظمة عند الضرورة، وكذلك التأكد من ضمان استمرارية الاستغلال بتوافر الإجراءات البديلة الخاصة بالمعلوماتية لدى البنوك والمؤسسات المالية، وذلك عند حدوث أي طارئ، كما رسمت المادة 19 محيط مراقبة الأنظمة المعلوماتية إلى حفظ المعلومات والتوثيق الخاص بالتحاليل والبرمجة وبتنفيذ المعالجات (النظام 02-03، 2002).

وبذلك أطر النظام 02-03 من خلال المادة 18 و19، سبل مراقبة نظم المعلومات المستعملة بشكل رئيسي في تقديم خدمات الصيرفة الإلكترونية، إلا أنه لم يمس كل ما جاءت به وثيقة لجنة بازل المتعلقة بالرقابة على الصيرفة الإلكترونية لسنة 2001م، ذلك أن الجزائر لم تشهد في هذه المرحلة ولوجاً معتبراً لخدمات الصيرفة الإلكترونية داخل البنوك والمؤسسات المالية العاملة فيها، وكان استعمال نظم المعلوماتية مقتصراً بشكل كبير على خدمات الصيرفة التقليدية، لاسيما فيما يخص التقييد المحاسبي وعملية تخزين وحفظ المعلومات.

2.2- النظام رقم 11-08 المؤرخ في 28 نوفمبر 2011م، المتعلق بالمراقبة الداخلية للبنوك والمؤسسات المالية:

لقد صدر هذا النظام بهدف تحديد مضمون المراقبة الداخلية الواجب وضعها من قبل البنوك والمؤسسات المالية في ظل الأمر رقم 03-11 المؤرخ في 26 أوت 2003م، والمتعلق بالنقد والقرض، ولقد كرست كل من المادة 35 والمادة 36 من هذا النظام ما جاءت به كل من المادة 18 والمادة 19 من النظام 02-03 (المتعلق بالمراقبة الداخلية للبنوك والمؤسسات المالية)، وحملت إضافة جديدة على المادة 19 من النظام 02-03، فنصت المادة 36 من النظام 11-08 على الحفاظ على سرية ونزاهة المعلومات، وبهذا زادت دائرة القواسم المشتركة الخاصة بمسايرة الجزائر لتقرير لجنة بازل لإدارة المخاطر الرئيسية للصيرفة الإلكترونية في صيغته الجديدة لشهر جويلية 2003م.

وتأتي هذه الخطوة كإجراء لتفعيل الرقابة المصرفية على الصيرفة الإلكترونيية في الجزائر، وحماية خصوصية العميل والمستفيد من تلك الخدمات.

وجاء في النظام 11-08 عبر المادة 60، إلزاماً للبنوك والمؤسسات المالية بتسجيل الحوادث المعتبرة الناجمة عن تقصير في احترام أو صياغة الإجراءات الداخلية، وعن الاختلالات في الأنظمة لاسيما المعلوماتية، التي ترتبط بشكل كبير بالعمل المصرفي الإلكتروني، كنا أنها فسحت المجال أمام البنوك والمؤسسات المالية بتحديد المعايير الملائمة لتسجيل طبيعة مخاطرها ونشاطاتها، ووضعت أيضاً مجموعة من الاعتبارات، على ضوئها يتم وضع ملف أو

ملفات الحوادث تحت تصرف المسؤولين عن الرقابة الدائمة والدورية، كما ألزمت المادة 62 من النظام البنوك والمؤسسات المالية، بإعداد مجموع وثائق تحدد بدقة الوسائل الموجهة لضمان السير الحسن لجهاز الرقابة الداخلية، لاسيما الإجراءات المتعلقة بأمن أنظمة المعلومات والاتصال، وهذا أيضاً له ارتباط وثيق بالصيرفة الإلكترونية، ومنه يمكن القول أن المادة 60 والمادة 62 من النظام 11-08، اهتمت بتفعيل الرقابة المصرفية على النظم المعلوماتية التي تعتبر عنصراً أساسياً لتقديم خدمات الصيرفة الإلكترونية.

3.2- النظام رقم 05-07 المؤرخ في 28 ديسمبر 2005 المتضمن بأمن أنظمة الدفع:

هدف النظام رقم 05-07 المؤرخ في 28 ديسمبر 2005م المتعلق بأمن أنظمة الدفع إلى تعريف أنظمة الدفع، وجهاز الأمن الخاص بها، ولقد صدر بعد النظام رقم 05-04 المتضمن نظام التسوية الإجمالية الفورية للمبالغ الكبيرة والدفع المستعجل، والنظام رقم 05-06 المتضمن مقاصة الصكوك وأدوات الدفع الخاصة بالجمهور العريض الأخرى، ومن خلال هذا النظام تعين على المشاركين والمسيرين لأنظمة الدفع، وضع أجهزة أمن حسب كل واحد منهم، تكون هذه الأجهزة مطابقة للمقاييس الدولية المعمول بها في هذا الشأن، كما وضح النظام 05-07 أن أمن أنظمة الدفع يتكون من أمن البنية الأساسية لأنظمة الدفع، وكذا أمن وسائل الدفع، وكذلك تعيين موظفين مؤهلين وأكفاء للقيام بعمليات الدفع، ولقد شدد هذا النظام على المشاركين في أنظمة الدفع بضرورة ضمان سرية وصحة المعلومات التي تمر عبر أنظمة الدفع، وكذلك إلزامية وضع أنظمة نجدة (Back-up) وتوفير موارد بشرية ملائمة بغرض ضمان استمرارية الاستغلال، مواجهةً لكوارث مفاجئة تحول دون الاشتغال العادي للمنشئات الأساسية، وألقى هذا النظام مسؤولية توفير الأمن للبنية الأساسية الخاصة بأنظمة الدفع واحترام المعايير المطبقة في هذا المجال لبنك الجزائر، كما أوضح لهذا الأخير حالة تعذره عن ذلك، أن يطلب من الجهة المصدرة اتخاذ التدابير اللازمة، أو توقيف إدخال وسيلة الدفع المعنية في النظام، حالة عدم تطبيق هذه التوصيات والتدابير، وأضاف على ذلك وبصفة خاصة على بنك الجزائر التأكد من أمن بطاقات الدفع، ومتابعة إجراءات توفير شروط الأمن المتخذة من قبل الجهات التي تصدرها، ويتضح من خلال النظام 05-07 المتضمن أمن أنظمة الدفع أن الجزائر حاولت أن تساير المعايير الدولية للرقابة المصرفية على المصرفية الإلكترونية، والتي أشار لها تقرير لجنة بازل شهر جويلية 2003م، خاصة ما تعلق بالسرية وصحة المعلومات الخاصة بالعميل، وضمان استمرارية الاستغلال من خلال خطة طوارئ، لكن تبقى عدة نقط مظلمة كان من المفروض التطرق إليها، كما هو منصوص عليها في وثيقة لجنة بازل، ولقد ترك النظام 05-07 الباب مفتوحاً أمام أي تعديل أو توضيح في المادة 13، التي نصت على أن تحدد كيفيات تطبيق هذا النظام كلما دعت الضرورة أو الحاجة لذلك، عن طريق تعليمة يصدرها بنك الجزائر.

3. الخاتمة:

وبالتالي ما يلفت الانتباه في المنظومة المصرفية الجزائرية، ذلك الضعف في التشريع المنظم للرقابة المصرفية الإلكترونية، بالرغم من توفر معايير دولية، يمكن إتباعها واعتمادها بكل سهولة، ويمكن أن يرجع ذلك لعدة اعتبارات، منها الانتشار الواسع لخدمات الصيرفة التقليدية، خاصة المتعلقة بعمليات الدفع والسحب، ونقص ثقافة استعمال وسائل الدفع الإلكترونية عند المستهلك والتاجر، والتخوف من مصالح الضرائب بالنسبة للبائعين، والغياب الشبه التام للتجارة الإلكترونية، وأسباب أخرى تجعل من التشريعات قليلة، و تجعلها تمس فقط العمليات الممارسة داخل البنوك، كالمقاصة الإلكترونية للشيكات والحوالات، وRTGS، غالباً ما تكون هذه المعاملات المصرفية ما بين مؤسسات فيما بينها، أو بينها وبين الأفراد، وعمليات السحب عن طريق البطاقات البنكية، ما يجعل الحاجة لهذه التشريعات لا تتماشى بشكل كاف ومنسجم مع المستوى الرقابي العالمي للعمليات المصرفية الإلكترونية، وغير متأثرة بالسلوك المصرفي للعملاء الذين يقبلون بصفة أكثر على خدمات الصيرفة التقليدية في تعاملاتهم اليومية مقارنة بخدمات الصيرفة الإلكترونية، ويمكننا الخروج بجملة من التوصيات:

- تشجيع الإقبال على منتجات الصيرفة الإلكترونية، من خلال التأثير على السلوك المصرفي للعملاء.

- الاستغلال الأمثل للبنية التحتية التكنولوجية المتوفرة عبر الجزائر، وذلك لتوسيع انتشار الصيرفة الإلكترونية، وتقديم خدماتها بشكل يرقى إلى تطلعات العملاء.

- ضرورة مسايرة المنظومة المصرفية الجزائرية لوثيقة لجنة بازل المتعلقة بإدارة مخاطر الصيرفة الإلكترونية.

- ضرورة إصدار بنك الجزائر لتشريع خاص بالرقابة على الصيرفة الإلكترونية، كما هو الحال عليه في العديد من الدول، منها العربية كمصر مثلاً.

- الاستفادة من تجارب بعض الدول الرائدة في مجال الرقابة المصرفية على الصيرفة الإلكترونية، من بين ذلك بعض الدول العربية مثل السعودية والإمارات المتحدة.

- القيام بعملية الإفصاح عن الأنشطة المصرفية الإلكترونية من قبل البنوك التجارية وشركة SATIM، من أجل إدارة مخاطر الصيرفة الإلكترونية بأسلوب فعال وسليم.

- الاهتمام برأس المال البشري القائم بعملية إدارة مخاطر الصيرفة الإلكترونية، وذلك من حيث التكوين والتدريب بشكل يتناسق مع المعايير الدولية، ومتطلبات العمل المصرفي الإلكتروني.

- **قائمة المصادر والمراجع: (Simplified Arabic : 11)**

1- سارة سعيدة حركات بن عيدة. (2018). **إدارة مخاطر الصيرفة الإلكترونية وأثارها على الخدمة البنكية الإلكترونية**. مجلة العلوم الإنسانية لجامعة أم البواقي (العدد التاسع).

2-عبد الله محمد طاهر. (2015). **أطروحة دكتوراه: التأثير المتبادل بين الكتلة التقنية والصيرفة الإلكترونية**. كلية الاقتصاد، جامعة دمشق، سوريا.

3-وسيم محمد الحداد وآخرون. (2012). **الخدمات المصرفية الإلكترونية**.دار الميسرة. الأردن

4-الجريدة الرسمية عدد 84 مؤرخة في 18 ديسمبر 2002،**النظام 02-03. (14 نوفمبر, 2002).** المتضمن المراقبة الداخلية للبنوك والمؤسسات المالية.

5-الجريدة الرسمية عدد 47 مؤرخة في 29 أوت 2012،**النظام 11-08. (28 نوفمبر, 2011)**. المتعلق بالرقابة الداخلية للبنوك والمؤسسات المالية.

6-الجريدة الرسمية عدد 37 مؤرخة في 04 يونيو 2006،**النظام 05-07. (28 ديسمبر, 2005)**. المتضمن أنظمة الدفع.

7-Basel Committe, o. b. (july 2003). **Basel Committe on banking supervision Risk managment principles for elecronic. bank for international settleents**.

8-SOLANKI, V. S. (september2012). **RISK IN E-BANKING AND THEIR MANAGEMENT**. International jornal of marketing financial services and management research , vol1 (Issue9).