بن شريف مريم

المركز الجامعي خميس مليانة

مداخلة بعنوان:

الأعمال المصرفية الالكترونية الرهانات والتحديات- إشكالية الإشراف والرقابة المصرفية-

الملخص:

يشهد العالم الآن تحولا في مجالات عدة، وساعد في هذا التطور تطور أجهزة المعلوماتية على مختلف أشكالها، بما يمكن من تناقل المعلومات عبر الشبكات وبوسائل متناهية في الصغر، كأجهزة الحاسوب المتنقلة ووسائل التخزين المتعددة كالبطاقة الذكية التي تحملا جهاز حاسوب مكتمل.

تأتي هذه الورقة لتسليط الضوء على بعض القضايا الشائكة المتعلقة بالصيرفة الالكترونية، منها المخاطر المصرفية الالكترونية وكيفية إدارتها، إشكالية الرقابة والإشراف على الأعمال المصرفية الالكترونية ومدى أمن هذه العمليات.

إذ أن البنوك الالكترونية تتعرض نتيجة أدائها لمهامها لمجموعة من المخاطر التي تستوجب وضع إجراءات حكيمة لإدارتها والحد منها في سبيل تحقيق الاستقرار المصرفي و من ثم الاستقرار المالي.

وهذا ما يطرح مجموعة من التحديات أمام الهيئات المكلفة بالإشراف والرقابة وفقا لمقررات لجنة بازل، وذلك نتيجة للانتشار الواسع للبنوك الالكترونية والسرعة الفائقة التي تنمو بها الأعمال المصرفية الالكترونية.

لذلك يجب تكثيف الجهود من طرف كل الهيئات المعنية إلى جانب هيئات الإشراف والرقابة لتعزيز الرقابة على مخاطر هذه العمليات وكذا السعي لتوفير أمن هذه العمليات من هجمات التجسس والتصيد.

Abstract :

Now the world is witnessing a shift in several areas, and helped in the development of IT hardware development on various forms, including possible transmission of information through networks and by means of micro, such as computers and deferent means of stockage such as smart card.

This paper is to shed light on some thorny issues relating to electronic Banking, including the risks of electronic banking and how to manage, the problem of control and supervision of electronic banking and the security of these operations.

As a result of electronic banking are the performance of its functions to a range of risks that require prudent procedures to manage and reduce them in order to achieve stability of the banking and financial stability then.

This poses a series of challenges before the bodies charged with overseeing and supervision in accordance with the decisions of the Basel Committee, as a result of the widespread existence of banks, electronic and high speed are growing e-banking.

We must therefore intensify efforts by all concerned bodies to the bodies of supervision and control to enhance control of the risks of these operations, as well as seeking to provide the security of these operations from piracy.

مقدمة:

تعتبر البنوك الالكترونية صوت المستقبل، إذ أنها توفر فوائد كثيرة جدا للمتعاملين بعرض عمليات سهلة وأقل تكلفة، ولكنها تطرح كذلك مشاكل جديدة للهيئات المشرفة فيما يتعلق بالقوانين والتنظيمات والرقابة على النظام المالي، وكذا بالنسبة لوضع وتطبيق السياسة الاقتصادية الكلية.

إذ أن البنوك الالكترونية أدت نتيجة انتشارها الواسع إلى زيادة درجة المخاطر مما يطرح إشكالية إدارة هذه المخاطر ، وهذا بالإضافة إلى أنهه هل أن هذه الأعمال المصرفية تتميز بالأمن أم لا ، وهذا ما سنتطرق إليه في هذه الورقة ، وذلك بالإجابة على التساؤل التالي:

"في ظل المخاطر المتزايدة علاوة على المخاطر المصرفية التقليدية، كيف يمكن لهيئات الرقابة والإشراف أن تمارس عمليات الرقابة والإشراف على الأعمال المصرفية الالكترونية؟ وما مدى أمن الأعمال المصرفية الالكترونية؟"

أولا: مفهوم العمليات المصرفية الالكترونية:

يستخدم اصطلاح المصارف الالكترونية (E-banking) كتعبير متطور وشامل للمفاهيم التي تبلورت مع بداية التسعينات مثل : المصارف عن بعد، المصارف الافتراضية، المصارف على الخط، المصرف المنزلي ومصارف أخرى تقدم خدمات مصرفية الكترونية بالإضافة إلى عملها بالطرق التقليدية.[01]

فالمقصود بالصيرفة الالكترونية هو إجراء العمليات المصرفية بطرق الكترونية[02] أي باستخدام تكنولوجيا الإعلام والاتصال الجديدة سواء تعلق الأمر بالسحب أو الدفع أو الائتمان أو التحويل أو بالتعامل

في الأوراق المالية، وغير ذلك من الأعمال المصرفية حيث يمكن للزبون القيام بإدارة حساباته وإنجاز أعماله المتصلة بالبنك عن طريق المنزل أو المكتب أو أي مكان آخر وفي الوقت الذي يريده.[03]

إذ أن الاتجاه السائد من طرف أنظمة خدماتية كثيرة بما فيها البنوك هو الإحلال الجزئي للآلة بدل العنصر البشري أي الأتمتة Automatisation إذ تتمثل أهم صورها فيما يلي:[04]

1- النقود الالكترونية:

يصدرها البنك في شكل وسائط تحتوي على شرائح ممغنطة وتدعى ببطاقات القيمة المخزنة يقابلها مقدار من الوحدات النقدية بحيث توضع تحت تصرف الزبون للتعامل مع جهاز الصرف الآلي من أجل السحب النقدي أو لطلب كشف الحساب ودفتر الشيكات وكذا تحويل الأموال وغيرها وهذا على مدار 24 ساعة.

2- البنك المنزلي:

يتم تحميل الحاسوب الشخصي ببرنامج خاص يوفره البنك مجانا أولقاء رسوم للزبائن لأغراض الإطلاع على الحساب والتصرف في أرصدة الحسابات المصرفية عن طريق خط خاص يبدأ طرفه من المكتب أو المنزل أو أي مكان وفي أي وقت وينتهي طرفه الثاني عند الحاسوب المركزي للبنك.[05]

3- الخدمات المصرفية التلفونية:

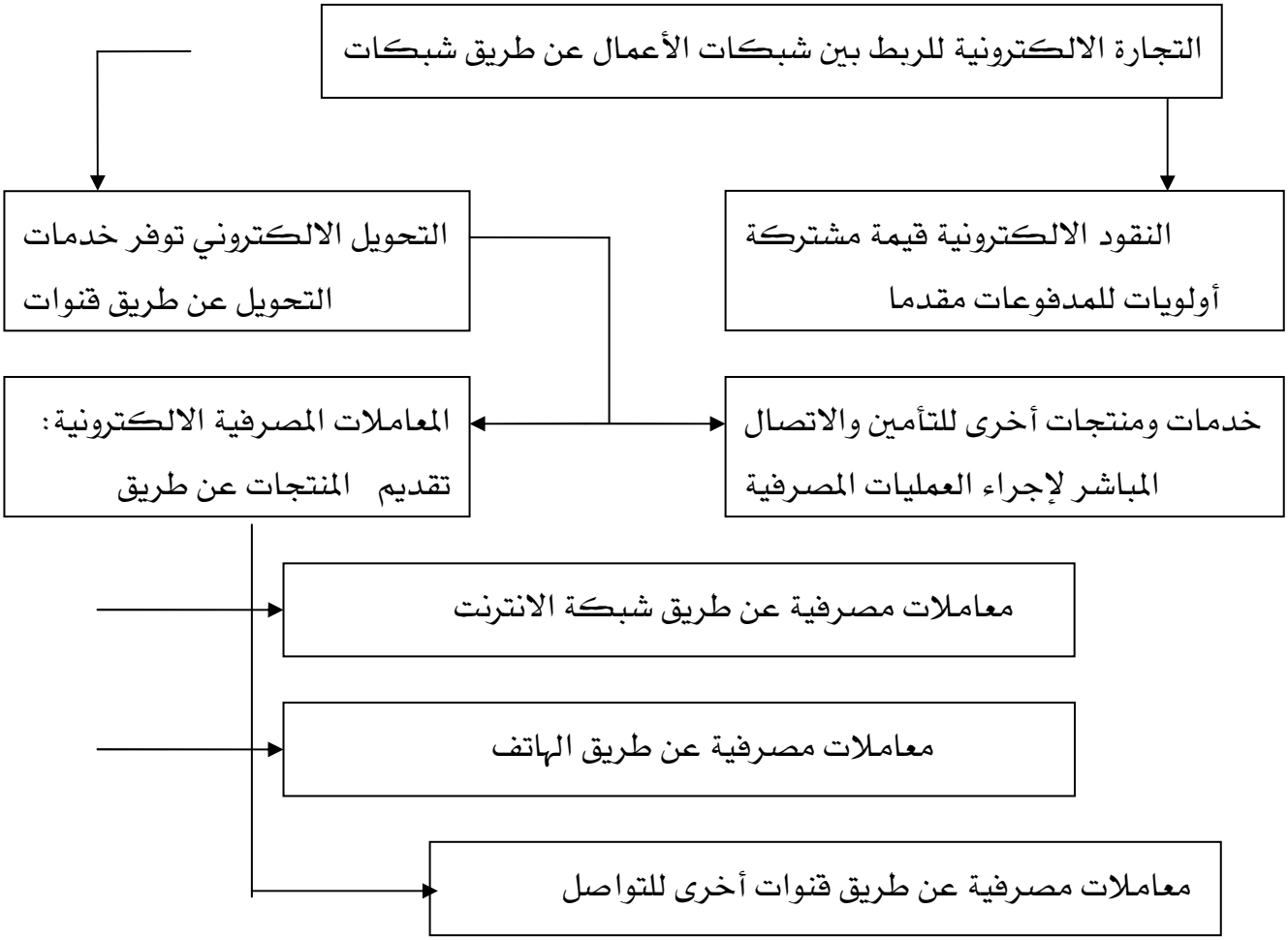
حيث تكون خدمة الزبائن عبر جهاز التلفون لاسيما الجوال على مدى 24 ساعة، ووفق سياق منظم يحدد الزبون من البرنامج الصوتي الذي يشتغل بمجرد الاتصال بأرقام خاصة وضعها البنك في متناول عملائه نوع الخدمة المصرفية التي يريدها.

وتتمثل مزايا العمليات المصرفية الالكترونية فيما يلي:[06]

- إمكانية وصول البنوك إلى استقطاب اكبر عدد من العملاء المودعين والمقترضين وطالبي الخدمات المصرفية.
- تحديث الخدمات المصرفية
- تخفيض تكاليف التشغيل بالبنوك وتكاليف إنجاز عمليات التجزئة محليا ودوليا.

و نلخص صور المعاملات المصرفية الالكترونية في الشكل الآتي:

شكل رقم (01): صور المعاملات المصرفية الالكترونية



المصدر: جاسم السنوسي ، " المصارف الالكترونية" مقال منشور على الانترنت على الموقع:
www.Bank.Of.cd.com 19/02/2011

ثانيا: مخاطر العمليات المصرفية الالكترونية:

يصاحب تقديم العمليات المصرفية الالكترونية مخاطر متعددة حيث أشارت لجنة بازل للرقابة المصرفية إلى ضرورة قيام البنوك بوضع السياسات والإجراءات التي تتيح لها إدارة هذه المخاطر من خلال تقييمها والرقابة عليها ومتابعتها، إذ تمحورت هذه المخاطر حول مخاطر التشغيل، السمعة، الائتمان، السيولة، سعر الفائدة، السوق، ومخاطر قانونية وذلك على النحو التالي:

1- **مخاطر التشغيل**: Operational Risk

تنشأ المخاطر التشغيلية مما يلي:[07]

أ) عدم التأمين الكافي للنظم: System Security

وينتج عن عدم إمكانية اختراق غير المرخص لهم لنظم حسابات البنك بهدف التعرف على الخاصة بالعملاء واستغلالها سواء تم ذلك من خارج البنك أو من العاملين به، لذلك يجب توافر إجراءات كافية لكشف وإعاقة هذا الاختراق.

ب) عدم ملائمة تصميم النظم أو إنجاز العمل أو أعمال الصيانة:

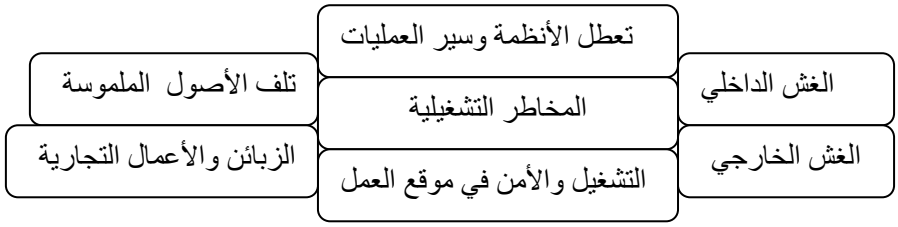
وتنشأ من إخفاق النظم أو عدم كفاءتها لمواجهة متطلبات المستخدمين وعدم السرعة في حل المشاكل وصيانة النظم وخاصة إذا زاد الاعتماد على مصادر خارج البنوك لتقديم الدعم الفني بشأن البنية الأساسية اللازمة.

ج) إساءة الاستخدام من قبل العملاء:

ويكون ذلك نتيجة عدم إحاطة العملاء بإجراءات التأمين الوقائية.

ونورد فيما يلي شكلا توضيحيا لمركبات المخاطر التشغيلية لدى البنوك وفقا لمقررات لجنة بازل.

الشكل رقم (02): مركبات المخاطر التشغيلية لدى البنوك وفق لجنة بازل



المصدر: حمزة طيبي، عبد الرزاق خليل: إدارة مخاطر العمليات المصرفية الالكترونية وفق معايير لجنة بازل مقال منشور على الانترنت http://www.shatarat.net.19/02/2011

2/ مخاطر السمعة:

تنشأ مخاطر السمعة في حالة توافر رأي عام سلبي تجاه البنك الأمر الذي قد يمتد إلى التأثير على بنوك أخرى نتيجة عدم مقدرة البنك على إدارة نظمه بكفاءة أو حدوث اختراق مؤثر بها.

3/ المخاطر القانونية:

تحدث هذه المخاطر في حالة عدم احترام القوانين أو القواعد أو الضوابط المقررة خاصة تلك المتعلقة بمكافحة غسيل الأموال أو نتيجة عدم التحديد الواضح للحقوق والالتزامات القانونية الناتجة عن العمليات المصرفية الالكترونية ومن ذلك عدم وضوح ما إذا كانت هناك قواعد لحماية المستهلكين في بعض الدول أو لعدم المعرفة القانونية لبعض الاتفاقيات المبرمة باستخدام وسائل الوساطة الالكترونية.(08)

4- مخاطر أخرى:

كما هو الحال بالنسبة للمخاطر الخاصة بالعمليات المصرفية التقليدية فإن العمليات المصرفية الالكترونية تواجه كذلك مخاطر الائتمان، السيولة، سعر الفائدة ومخاطر السوق، حيث أن قنوات حديثة للاتصال بالعملاء وامتداد نشاط منح الائتمان إلى عملاء عبر الحدود قد يزيد من احتمالات إخفاق بعض العملاء في سداد التزاماتهم.(09)

ثالثا: المبادئ الاسترشادية لإدارة المخاطر:

تشتمل إدارة المخاطر على التقييم، الرقابة والمتابعة وذلك على النحو التالي:(10)

1- **تقييم المخاطر**: Assessing Risks

وذلك من خلال تحديد المخاطر التي قد يتعرض لها البنك، ومدى تأثيرها عليه وكذا وضع حدود قصوى لما يمكن للبنك ان يتحمله من خسائر نتيجة التعامل مع هذه المخاطر.

2- الرقابة على التعرض للمخاطر:

وتشتمل هذه الرقابة على ستة مجالات وذلك على النحو التالي:

أ) تنفيذ سياسات وإجراءات التأمين:

وتستهدف هذه السياسات مايلي:

1 - تحديد شخصية المتعامل مع النظم.

2- ضمان عدم إجراء تعديلات على رسائل العملاء أثناء انتقالها عبر القنوات.

3- ضمان الحفاظ على سرية معاملات العملاء.

4- ضمان عدم إنكار مرسل الرسالة لها.

ويراعى في هذا المجال مايلي:

1) إتباع سياسات وإجراءات تحقق تأمين الاتصالات من وإلى النظم لمنع أو الحد من اختراق غير المرخص لهم للنظم أو إساءة استخدامها.
2) الرقابة على دخول النظم وتحديد شخصية المستخدمين.
3) حماية النظم من احتمالات القيام بممارسات غير مرخص بها من قبل العاملين بالبنك السابقين أو الجدد أو المؤقتين.

ويتطلب الأمر بالنسبة لإصدار وسائل لنقود الكترونية اتخاذ إجراءات إضافية للتأمين ويشمل ذلك:

- الاتصال المباشر على مصدر البطاقات أو المشغل المركزي للحماية من التزييف.
- متابعة العمليات الفردية.
- الاحتفاظ بقاعدة بيانات مركزية لتتبع عمليات غسيل الأموال.
- توافر شروط الأمان في البطاقات الذكية، أو غيرها مع مراعاة وضع حد أقصى لما يخزن على البطاقة.

ب) تدعيم الاتصالات بين المستويات المختلفة بالبنك من مجلس إدارة وإدارة عليا وبين العاملين بشأن سلامة أداء النظم وتوفير التدريب المستمر للعاملين.

ج) استمرار تقديم وتطوير الخدمات.

د) وضع ضوابط للحد من المخاطر في حالة الاعتماد على مصادر خارج البنك لتقديم الدعم الفني وتشتمل هذه الضوابط على مايلي:

- متابعة الأداء المالي والتشغيلي لمقدمي الدعم الفني.
- التأكد من توافر اتفاقيات تعاقدية مع مقدمي الدعم الفني تحدد التزامات الأطراف تفصيليا في حالة تعرفهم على بيانات

ذات حساسية تخص البنك، وذلك من خلال مراجعة سياساتهم وإجراءاتهم في هذا المجال.

- توفير ترتيبات طوارئ لتغطية احتمالات حدوث تغيير مفاجئ في مقدمي الدعم الفني.

ه- إحاطة العملاء عن العمليات المصرفية الالكترونية وكيفية استخدامها.

و- إعداد خطط طوارئ بديلة في حالة إخفاق النظم عن أداء الخدمات.

3) متابعة المخاطر:

تتمثل متابعة المخاطر في اختبار النظم وإجراء المراجعة الداخلية والخارجية وذلك على النحو التالي:

أ) إجراء اختبارات دورية للنظم:

والتي يكون من ضمنها:

- إجراء اختبار إمكان الاختراقPenetration Testing الذي يهدف إلى تحديد وعزل وتعزيز تدفق البيانات من خلال النظم و اتباع إجراءات لحماية النظم من المحاولات غير العادية للاختراق.
- إجراء مراجعة دورية من خلال النظم للتأكد من فاعلية إجراءات التأمين والوقوف على مدى اتساقها مع سياسات وإجراءات التأمين المقررة.

ب) إجراءات المراجعة الداخلية والخارجية:

تسهم المراجعة الداخلية والخارجية في تتبع الثغرات وحالات عدم الكفاءة وتخفيض حجم المخاطر بهدف التحقق من توافر سياسات وإجراءات مطورة والتزام البنك بها.

رابعا: الضوابط الرقابية للعمليات المصرفية الالكترونية:

سنتطرق إلى هذه الضوابط من خلال إلزامية حصول البنوك على ترخيص لتقديم العمليات المصرفية الالكترونية، أسبابه وكذا شروط الحصول عليه.[11]

أ- أسباب حصول البنوك على ترخيص لممارسة العمليات المصرفية الالكترونية:

هناك عدة أسباب تستلزم حصول البنوك على ترخيص لتقديم العمليات المصرفية الالكترونية نذكر منها:

1- حماية السوق المصرفي المحلي من مقدمي الخدمات المصرفية غير المرخص لهم من طرف البنك المركزي بتقديم هذه الخدمات بما في ذلك الجهات التي ترغب في تأسيس كيان مستقل لا توجد له فروع مادية بغرض تقديم العمليات المصرفية الالكترونية فقط Virtual Bank.

2- التحقق من توافر الوسائل الكافية لدى البنوك للإدارة الحصيفة لمخاطر تلك العمليات.

3- تطبيق الضوابط الرقابية اللازمة لحصول البنوك على ترخيص لتقديم هذه العمليات.

ب) شروط حصول البنوك على ترخيص:

يشترط حصول البنوك على الترخيص مايلي:

1- يقتصر منح الترخيص على البنوك المسجلة لدى البنك المركزي فقط.

2- التزام البنك بكل من معيار كفاية رأس المال وأسس تصنيف القروض وتكوين المخصصات والتوازن في مراكز العملات والتركز الائتماني.

3- أن يتبع البنك مبادئ حصيفة لإدارة مخاطر تقديم خدماته من خلال شبكات الاتصال الالكترونية والتي تشمل على تقييم المخاطر والرقابة عليها ومتابعتها.

4- أن يحدد البنك نوعية الخدمات التي سيقوم بتأديتها من خلال الشبكات.

5- أن يحدد البنك المسؤوليات الواقعة على العميل من جراء حصوله على الخدمات عبر الشبكات.

6- إفصاح البنك المرخص له بالقيام بالعمليات المصرفية الالكترونية، رقم وتاريخ الحصول عليه، مع ربط الموقع بصفحة البنك المركزي المعلن فيها عن أسماء البنوك المرخص لها بذلك حتى يتحقق العملاء من صحة الترخيص.

خامسا :العمليات المصرفية الالكترونية؛ مشاكل جديدة بالنسبة لهيئات الرقابة والإشراف:

نتج عن العمليات المصرفية الالكترونية مشاكل وتحديات بالنسبة لهيئات الرقابة والإشراف أهمها يتعلق بالنمو السريع لهذه العمليات وذلك بأقل تكلفة وسهولة اعتمادا على التكنولوجيا لضمان أمن العمليات البنكية مثلما أن الانترنت يسمح بتوفير الخدمات في كل مكان في العالم، فالبنوك تعمل على التهرب من القوانين والرقابة. فماذا يمكن أن تفعل هيئات الرقابة والإشراف؟[12]

يمكن للهيئات المكلفة بالإشراف والرقابة أن تجبر حتى البنوك التي تقدم خدمات مصرفية عن بعد بإلزامية الحصول على اعتماد لممارسة العمليات المصرفية الالكترونية، وتقديم كل المعلومات المتعلقة بمكان البنك ومختلف الخدمات التي يقدمها.

كما أنه على البنوك الالكترونية احترام والالتزام بكل التشريعات المنظمة لعملها.

أ) الإجراءات المتخذة من طرف هيئات الرقابة والإشراف:

ولتفادي مساوئ البنوك عن بعد يجب على هيئات الرقابة والإشراف أن تركز على أربعة نقاط أساسية نذكرها فيما يلي:

1- **التكييف**:Adaptation

نتيجة سرعة التطور التكنولوجي وأثرها على العمليات المصرفية، أصبحت عملية الإشراف والرقابة مهمة صعبة للغاية وتحتاج إلى وقت، ففي ماي 2001 نشر بنك التسويات الدوليةBRI مقال بعنوان "مبادئ إدارة مخاطر الصيرفة الالكترونية" "Risk Management Principles For Electronic banking " موضحا كيفية تكييف وتوسيع إطار فعلي لتسيير مخاطر البنوك الالكترونية ، كما يوصي بنك التسويات الدولية بأنه مثلا على مجلس الإدارة والإطارات السامية للبنك أن تختبر وتظهر المبادئ الأساسية لعملية الرقابة والحماية التي يجب أن تتضمن معايير للتأكد من صحة هوة العميل، بالإضافة إلى ترقية العمليات وضمان نزاهتها .

كما أنه على هيئات الرقابة والإشراف أن تسهر على أن يمتلك أعوانها الكفاءات التكنولوجية اللازمة للتمكن من تقييم تطور المخاطر المتعلقة بالأعمال المصرفية الالكترونية أي عليها الاستثمار الرفيع المستوى في المعلومة، وأجهزة الإعلام الآلي والبرمجيات.

2- **التصديق**:Légalisation

الإجراءات الحديثة وآليات تقديم الخدمات يجب أن تكون محددة ومعروفة قانونا ومعتمدة. فمثلا بالنسبة للتوقيع الالكتروني يجب أن يكون محددا وأن تمنح له نفس القيمة القانونية مثله مثل التوقيع المكتوب يدويا ، كما أنه يجب إعادة النظر في المفاهيم القانونية للبنك الالكتروني ومفهوم الحدود الوطنية.

3- التنسيق والتوافق: Harmonisation

يعتبر كل من التنسيق والتوافق الدولي فيما يخص قانون البنوك الالكترونية من الأولويات أي التعاون المتبادل بين هيئات الرقابة من خلال وضع تقنين بنكي الكتروني على المستوى الدولي والمحلي.

ضف على ذلك أن مشكل الكفاءة في العمليات بلا حدود لم يحل بعد.

إذ أن كل بلد عليه اتخاذ القرارات المناسبة لاختيار من هو كفء لوضع القوانين المنظمة للبنوك الالكترونية.

ولكن ماهو موجود هو أن التنسيق والتوافق والتعاون تعد من أصعب التحديات التي تواجه في مجال البنوك الالكترونية.

4- **الدمج والتكامل:**Intégration

أي إدراج تكنولوجيا المعلومات والمخاطر التشغيلية في تقييمات الأمن والحماية الموفرة من طرف هيئات الرقابة البنكية.

فيما يخص مسائل الثقة والأمان يجب على هيئات الرقابة أن تجبر البنوك على توضيح كيفية وضع برنامج أعمال البنك الالكتروني ويتعلق الأمر خاصة بالوظائف الموقعة في الخارج.

ب) رهانات البنوك الالكترونية على مستوى الاقتصاد الكلي:

إن هيئات الإشراف والتنظيم ليست وحدها المعنية بالتحديات التي تطرحها البنوك الالكترونية، حيث أن البنك الالكتروني يغير بسرعة صورة النظام المالي ويزيد من احتمالات التحويل السريع لرؤوس الأموال من بلد لآخر، إذ أن متخذي القرار فيما يخص السياسات الاقتصادية الكلية يواجهون قضايا جد صعبة منها:

- إذا كان البنك الالكتروني لا يولي أهمية للحدود الوطنية من خلال تسهيل حركة رؤوس الأموال، فماهي نتائج ذلك على السياسات الاقتصادية الكلية؟
- كيف يتم وضع السياسة النقدية إذا كان استعمال الطرق الالكترونية يسمح بسهولة للبنوك بتجاهل الاحتياطات الإجبارية ، أو أن العمليات يمكن تنفيذها بالعملة الأجنبية أو بالعملة الوطنية؟
- عندما تكفي مجرد نقرات للفأرة للحصول على خدمات بنكية أوفشور (خارج الحدود)، أو من إخراج رؤوس أموال بلد ما، تبعا لذلك هل تملك دولة ما هامش إدارة ميزاني أو نقدي؟
- ما مدى تأثير البنك الالكتروني في اختيار نظام سعر الصرف والمستوى المستهدف للاحتياطات الخارجية للبنك المركزي؟
- الانتشار الواسع للبنوك الالكترونية هل يفرض انضباطا صارما للسوق في مختلف الدول أو حتى بالنسبة للمؤسسات؟

❖ يمكن مناقشة هذه القضايا من منظورين:

❖أولا: الثورة التكنولوجية خاصة الانتشار الواسع للنقود الالكترونية وبشكل عام التطورات الالكترونية للعمليات البنكية يمكن أن ينتج عنها توافق بين قرارات العائلات، المؤسسات والعمليات المالية للبنك المركزي، مما يعرض للخطر قدرة السياسة النقدية على التأثير في معدلات التضخم، وبشكل عام على الأهداف التي تصبو إليها من أجل الوصول إلى تحقيق الاستقرار المالي، كما أن السياسات الاقتصادية تواجه أيضا هذا التحدي.

❖ ثانيا: توسع البنوك الالكترونية يمكن أن يوفر انخفاضا صافيا في تكاليف المعاملات مما يكثف حركات رؤوس الأموال، مما يجعل السياسة النقدية تفقد فعاليتها.

وعليه لاتزال التحديات التي تطرحها البنوك الالكترونية قائمة سواء بالنسبة للسلطات النقدية وحتى الاقتصادية بشكل عام.

سادسا: أمن الأعمال المصرفية الالكترونية:

حاليا هناك الكثير من التهديدات التي تواجه العمليات المصرفية الالكترونية وأكثرها وضوحا هي غارات التصيد والبرامج الضارة.

أ) التصيد في الأعمال المصرفية الالكترونية:

التصيد هو[13] أحد الأنشطة غير القانونية ويمثل محاولات الحصول على معلومات شخصية وسرية مثل: اسم المستخدم، كلمة المرور، أرقام بطاقات الائتمان، الأرقام السرية للبطاقات...الخ عن طريق الخداع بإرسال رسائل بريد مزيفة يدعي فيها مرسلوها بأنهم مؤسسات شرعية.

إن هجمات التصيد غير موجهة نحو البنوك بل هي إلى عملاء البنوك، الأشخاص الذين يملكون حسابات في البنوك ويستعملون خدمات الأعمال المصرفية الالكترونية.

أحد اتجاهات التصيد في عام 2010 أظهرت تباين نمو المؤسسات المنتحلة والعملاء المستهدفين، كنتيجة مباشرة للأزمة الاقتصادية، وهكذا كانت المؤسسات الاقتصادية الهدف المفضل لمجرمي الانترنت مع أكثر من 70 %[14] من رسائل هجمات التصيد، معظم رسائل التصيد التي انتشرت خلال النصف الأول من عام 2010 كانت مكتوبة باللغة الانجليزية

- 75% من هذه الرسائل تمت معالجتها من قبل- تلتها اللغة الفرنسية 13% والسويدية 3 %، واحتلت الروسية المرتبة الرابعة بمعدل2 % تقريبا، في حين احتلت Bit Defender المرتبة الأخيرة من الرسائل غير المرغوب فيها مكتوبة باللغة البلغارية ب0.42 % من رسائل الاحتيال العالمي.

قائمة أكثر من 10 هويات مزورة في النصف الأول من عام 2010[15]

Paypal	53%
eBay	15%
HSBC	10%
Facebook	7%
IRS	4%

	3%
VISA	
Mastercard	3%
Bank of America	2%
Poste Italienne	1%
EGG	1%

حصان طراودة المصرفي يمثل سلالة من البرامج الخبيثة على عكس جواسيس المفاتيح(كي لوجر) القادرة على اعتراض وإرسال كل مفتاح يقوم المستخدم بضغطه أمام الكمبيوتر،فإن حصان طراودة المصرفي قد صمم خصيصا ليبقى نائما معظم الوقت ويستيقظ فقط عندما يقوم المستخدم بدخول موقع لأحد البنوك الموجودة في قائمته للمراقبة فيقوم البرنامج الضار بتنفيذ خدع متنوعة لاعتراض المعلومات المدخلة وإرسالها إلى القاعدة.

إن هذا المستوى من السرية هو الذي يجعل حصان طراودة المصرفي صعب الإيجاد، ، وبما أنه يقوم فقط بتجميع بضع بايتات POST في كل جلسة، فإنه يكون قادرا على إرسال هذه البيانات إلى موقع المهاجم عبر تعليمة

حصان طراودة المصرفي لايقلق لوجود منافذ مغلقة أو جدار ناري فهو يحد بشكل كبير من فرص قيام مسؤول النظام بتحديد موقع الحزمة المارة على الشبكة ، الطريقة الوحيدة لمعرفة أن هناك شيئا خاطئا في هذه الحزم هي المراقبة الفعالة لحركة مرور الشبكة الصادرة من الجهاز من خلال إطار زمني قصير عندما يقوم المستخدم بزيارة مواقع الأعمال المصرفية الالكترونية ويضغط على الزر إرسال.

ب) موجة البريد المزعج داخل هجمات التصيد: (رسالة البريد الالكتروني الوهمية)

نشاطات التصيد تعتمد على نمط معين في العادة يقوم المتصيد بتوظيف أعدادا كبيرة من رسائل البريد المزعج لخداع المتلقين لتعمل على الكشف عن بيانات خاصة، في الظاهر تبدو هذه الرسالة كأنها مرسلة من طرف مؤسسة مصرفية وتطلب من عملائها الالتحاق برابط أو فتح صفحة ويب مرفقة.

معظم الحجج المرفقة في هذه الرسائل غير الشرعية هي غير صحيحة، على سبيل المثال؛ أن الحساب تم تعليقه أو انتهائه أو زيادة في رسوم السحب و طلب أن يتم تحديث البيانات لغايات أمنية، بعض الطرق الأخرى المستخدمة في الرسائل مثل أن يوعد المستخدم بمبلغ من المال إذا قام بتعبئة البيانات الخاصة به على النموذج على الانترنت أو النموذج المرفق، بكلا الحالتين يقوم المتصيدون باستخدام البيانات المستخرجة لإفراغ الحسابات البنكية بمحتوى دقيق يكرر تفاصيل المؤسسة المصرفية ، شكل الرسالة قد يختلف من صفحة، صورة، نص عادي.

أحد أحدث حملات التصيد والتي استهدفت عملاء الأعمال المصرفية الالكترونية وعملاء مواقع الدفع الالكتروني، قامت على استخدام العديد من المكونات الخبيثة مثلا: الرسالة غير المرغوب فيها التي تقوم بنشر البرامج الضارة التي تتضمن ترويج للحل الأمثل لمكافحة الفيروسات عبر برنامج مكافحة فيروسات مفتوح المصدر، وتطلب الرسالة من المستخدمين زيارة صفحة ويب لتحميل المنتج.[16]

ج) كيفية حماية الأموال من التجسس:

لأن رسائل البريد المزعجة تلعب دورا جوهريا في هجمات التصيد على المستخدم أن يكون على علم بالقواعد الواجب إتباعها عند التعامل مع الرسائل المرسلة من قبل المؤسسات الاقتصادية.

إذ ينبغي أن يولى اهتماما وثيقا لأساليب تحديد الهوية والتوثيق وينبغي أن ينظر إلى بعض العوامل الأمنية الأخرى لمنع العدوى الخبيثة وسرقة البيانات والمال عند الوصول إلى هذه الحسابات المصرفية الالكترونية.

ونذكر فيما يلي بعض النصائح لحماية الأموال من التجسس:

1- يجب عدم الرد على هذه الرسائل بإرسال أي بيانات شخصية(اسم المستخدم، كلمة المرور،رقم الحساب البنكي،رقم بطاقة الائتمان)، حتى لو كانت من مؤسسات اقتصادية أو اجتماعية أو تجارية تطالب المستخدمين للشبكة بتحديث بياناتهم لديها.معظم هذه المؤسسات لاترسل رسائل معنونة "إلى عزيزي المشترك" بل تقوم بتخصيصها على رسائلها (باسم العميل كاملا مع بعض تفاصيل تحديد الهوية) وتقوم بإرسالها عن طريق خدمات البريد الاعتيادية.

2- ترسل إليك نيابة عن مؤسسة اقتصادية ، لاتقدم أي معلومات حساسة على أي صفحة ويب يبدو شرعيا.

3- إذا كان لديك أي شك بشأن رسالة الكترونية وصلت إليك من قبل مؤسسات اقتصادية أتصل بهم مباشرة.

4- لاتضغط على أي رابط مرفق في في رسائل البريد المزعج(حتى روابط إلغاء التسجيل) لأنه قد يقوم بتشغيل برامج ضارة أخرى ويقوم بتعريض جهازك للخطر.

5- التأكد من أن برامج مكافحة التصيد يعمل على جهاز الكمبيوتر بالإضافة إلى أي برامج حماية أخرى قبل القيام بتصفح موقع الأعمال المصرفية الالكترونية.

6- يجب التأكد من أن موقع الويب المستقبل يستخدم تشفير رمز القفل.

7- تجنب استخدام جهاز كمبيوتر غير محمي، وإذا تلزم الأمر تأكد من استخدام أداة المسح.

8- لاتجري معاملاتك البنكية باستخدام أجهزة الكمبيوتر العمومية.

9- إذا تم استخدام اتصال لاسلكي، ينبغي التأكد من أن الاتصال آمن ومشفر مع وجود ثقة بصاحب نقاط الاتصال، وتجنب استخدام شبكة عامة غير آمنة عند إجراء المعاملات البنكية على الانترنت، وإذا اضطر لذلك ينبغي استخدام لوحة مفاتيح ظاهرية لإدخال البيانات الحساسة على الرغم من برامج جواسيس المفاتيح(كي لوجر) التقليدية.

خاتمة:

إذا كان للبنك الالكتروني فوائد بالنسبة للعملاء وإمكانيات تجارية جديدة للبنوك، فإنه يعمل على زيادة درجة المخاطر البنكية التقليدية.

وبالرغم من المجهودات المعتبرة التي كانت في كثير من الدول من أجل تكييف القوانين والرقابة البنكية فإنه يجب على الهيئات التنظيمية الإشرافية البقاء متيقظة إذ أنه من الضروري تقوية التنسيق والتوافق بين القوانين وكذا تعزيز التعاون الدولي في هذا المجال.

ومن جهة أخرى فإن السهولة التي تنتقل بها رؤوس الأموال من بنك لآخر ومن بلد لآخر بطريقة الكترونية تخلق إشكالية فيما يتعلق بتسيير السياسة الاقتصادية.

إذ أنه لفهم أثار البنوك الالكترونية فإنه على متخذي القرار بحاجة إلى أسس تحليلية صلبة.

كما ينبغي السعي لتوفير أمن الأعمال المصرفية الالكترونية من خلال مكافحة برامج الجوسسة والتصيد.

الهوامش:

(1) يوسف مسعداوي، البنوك الالكترونية،ملتقى المنظومة المصرفية الجزائرية والتحولات الاقتصادية – واقع وتحديات، كلية العلوم الإنسانية والعلوم الاجتماعية بجامعة الشلف، الجزائر 14 و15 ديسمبر 2004، ص 227.

(2) TOUFAIL ALISSAR, Adoption de la banque électronique et son impact sur cas du secteur du marché du LIBAN, la performance organisationnelle : mémoire présenté comme exigence partielle de la maîtrise en administration des affaires ;défusé sur Internet, http//www.yo pdf.eu.21/02/2011

(3) رحيم حسين، هواري معراج، الصيرفة الالكترونية كمدخل لعصرنة المصارف الجزائرية، ملتقى المنظومة المصرفية الجزائرية والتحولات الاقتصادية- واقع وتحديات- مقال منشور على الانترنت، http//iefedia.com.19/2011

(04) حمزة طيبي، عبد الرزاق خليل، إدارة المخاطر المصرفية الالكترونية وفق مقررات لجنة بازل الدولية، مقال منشور على http://www.shatarat.net.19/02/2011 الانترنت

(05) نفس المرجع (04)

(06) الضوابط الرقابية للعمليات المصرفية الالكترونية وإصدار وسائل دفع لنقود الكترونية، مقال منشور على الانترنت،
http://www.pheladelfia.edu.jo/courses.19/02/2011 .

(07) نفس المرجع السابق.

(08) نفس المرجع السابق.

(09) علي قابوسة، المصارف الالكترونية الفرص والتحديات حالة الجزائر، مقال منشور على الانترنت، http://iefedia.com/ arab. 19/02/2011.

(10) نفس المرجع السابق.

(11) الضوابط الرقابية للعمليات المصرفية الالكترونية، مرجع سابق.

(12) Salah M.Nsouli et Andrea Schaechter,les enjeux de la banque électronique,revu de Finance et Développement,decembre2002, p48.

(13) رزفان ليفتز، ترجمة روزين جمال، ما مدى أمن الأعمال المصرفية الالكترونية، مقال منشور على الانترنت،
http://www.security4arabs.com.19/01/2011.

(14) نفس المرجع السابق.

(15) نفس المرجع السابق.

(16) نفس المرجع السابق.