ندوة حول : الأمن الإلكتروني

مداخلة بعنوان :

دور أمن المعلومات في تفعيل نشاط الصيرفة الإلكترونية

سارة مولاي مصطفى*

جامعة المدية

الملخص :

تهدف هذه الورقة البحثية إلى تسليط الضوء على دور أمن المعلومات في تفعيل نشاط التجارة الإلكترونية عموما والصيرفة الإلكترونية خصوصا لاسيما مع بروز الفجوة الرقمية واستخدام وسائل تكنولوجيا المعلومات والاتصال في المصرف في حد ذاته ومدى مواكبته لما يحدث داخل أي منظومة مصرفية، لذا ستبحث هذه الدراسة في تحليل ودراسة مختلف العوامل التي تعمل على إرساء منظومة مصرفية إلكترونية تستجيب للمقاييس والمواصفات المتعلقة بضمان السرية والأمن لمختلف المعاملات والمعلومات الإلكترونية.

Summary:

This paper aims to shed light on the role of information security in activating the overall e-commerce and e-banking in particular, especially with the emergence of the digital divide and the use of information and communication technology in the bank itself and the extent of coping with what is happening within any banking system, so it will discuss this study in the analysis and the study of the various factors that are working to establish an electronic banking system responds to the standards and specifications relating to ensuring the confidentiality and security of the various transactions and electronic information.

* طالبة دكتوراه بكلية العلوم الاقتصادية والتجارية وعلوم التسيير ،جامعة يحي فارس بالمدية.

مقدمة:

تماشيا مع التطور التكنولوجي وبروز البنوك الإلكترونية إلى حيز الوجود اصطدمت هذه البنوك بالمشاكل التكنولوجية وعلى رأسها مشكلة القرصنة التي تعتبر أخطر جريمة اقتصادية تمس الحسابات المصرفية والتي تؤثر على نشاط المصرف وسمعته والتي تؤدي إلى انعدام الثقة فيه مما يهدد بقاءه في السوق، واستجابة للواقع الجديد ونتيجة للمشاكل المتكررة التي ظهرت إلى حيز الوجود مع التطبيقات المتكررة لنشاط المصارف الإلكترونية أصبح من الضروري البحث عن الحلول للمشاكل التي تعترض نشاط الصيرفة الإلكترونية من خلال اتخاذ مختلف التدابير الرامية للحفاظ على المعلومات والأجهزة والبرمجيات من كل عملية قرصنة قد تحدث بصفة غير قانونية وهو ما اصطلح على تسميته بتوفير أمن المعلومات الذي يسمح ببقاء البنك في ظل المنافسة القوية، وفي هذا السياق سنحاول في هذه الدراسة تحليل الإشكالية التالية: **ما هو دور أمن المعلومات في إعطاء الجودة والتميز لمنتجات الصيرفة الإلكترونية؟**

ولدراسة وتحليل هذه الإشكالية نبني دراستنا على الفرضية التالية: **جودة منتجات الصيرفة الالكترونية تتوقف على فاعلية الأنظمة المعلوماتية التي تضمن سرية الخدمة وإتاحتها في الوقت المناسب لطالبيها.**

ولمعالجة الإشكالية السابقة قسمنا هذه الورقة البحثية إلى ثلاثة محاور أساسية كما يلي:

المحور الأول: لمحة حول الصيرفة الإلكترونية؛

المحور الثاني: أمن المعاملات والمعلومات المصرفية الإلكترونية؛

المحور الثالث: أمن المعلومات ودوره في تفعيل نشاط الصيرفة الإلكترونية.

المحور الأول: لمحة حول الصيرفة الإلكترونية

تعد مسالة الإبداع والمنافسة في تكنولوجيا الخدمة رأس مال مصرفي لا يمكن الاستغناء عنه في الصناعة المصرفية ويبين منهج العلاقة بين المصارف التقليدية ومؤسسات الصيرفة الحديثة التي تتعامل مع زبائنها عن طريق شبكات الانترنت التي تسمح لها في عرض وتقديم منتجات مصرفية جديدة تمتاز بسهولة الاستخدام وسرعة وصولها إلى الزبائن إلكترونيا من خلال قناة توزيعِ الخدمات المالية بشكل جماعي تسمى الصيرفة الإلكترونية.

1. تعريف الصيرفة الإلكترونية:

الصيرفة الإلكترونية هي "تقديم الخدمات المصرفية باستعمال تكنولوجيا المعلومات والاتصال، أي من خلال الانترنت والموزعات الآلية والشبكات الخاصة والهاتف النقال والثابت والحاسب الشخصي، فهي تتيح الخدمة المصرفية عن بعد وخلال 24 ساعة وكل أيام الأسبوع وبسرعة فائقة وبتكلفة أقل وبدون التقاء مكاني بين العميل والمصرف"[1].

وجاء أيضا في مفهوم الصيرفة الالكترونية بأنها " إجراء العمليات المصرفية بطرق إلكترونية، أي باستخدام تكنولوجيا الإعلام والاتصال الجديدة، سواء تعلق الأمر بالسحب أو بالدفع أو بالائتمان أو بالتحويل أو بالتعامل في الأوراق المالية أو غير ذلك من أعمال المصارف"، وفي ظل هذا النمط من الصيرفة لا يكون الزبون مضطرا للتنقل إلى المصرف، إذ يمكنه القيام ببعض العمليات مع مصرفه وهو في منزله أو في مكتبه وهو ما يعني تجاوز بعدي المكان والزمان.

يتحدد مفهوم الصيرفة الإلكترونية بأنها " كافة العمليات أو النشاطات التي يتم عقدها أو تنفيذها أو الترويج لها من قبل المصارف والمؤسسات المالية بواسطة الوسائل الإلكترونية أو الضوئية مثل : الهاتف، والحاسب، والصراف الآلي، والإنترنت، والتلفزيون الرقمي وغيرها، وإلى جانب العمليات التي يقوم بها مصدرو البطاقات الإلكترونية، وكافة المؤسسات التي تتعامل بالتحويلات النقدية إلكترونياً"[2].

2. أنماط المصارف الإلكترونية وخدماتها:

ليس كل موقع لبنك على شبكة الانترنت يعني بنكا الكترونيا ، ووفقا للدراسات العالمية وتحديدا دراسات جهات الإشراف والرقابة الأمريكية والأوروبية ، فان هناك ثلاثة صور أساسية للبنوك الالكترونية على الانترنت [3]:

- **الموقع المعلوماتي** : وهو المستوى الأساسي للبنوك الالكترونية أو ما يمكن تسميته بصورة الحد الأدنى من النشاط الالكتروني المصرفي ، ومن خلاله فان البنك يقدم معلومات حول برامجه ومنتجاته وخدماته المصرفية.
- **الموقع التفاعلي أو الاتصالي**: بحيث يسمح الموقع بنوع ما من التبادل الاتصالي بين البنك وعملائه كالبريد الالكتروني , وتعبئة طلبات , أو نماذج على الخط , أو تعديل معلومات القيود والحسابات .
- **الموقع التبادلي**: وهذا هو المستوى الذي يمكن القول فيه ان البنك فيه يمارس خدماته وأنشطته في بيئة الكترونية ، حيث تشمل هذه الصورة السماح للعميل بالوصول إلى حساباته , وأدارتها,وأجراء الدفعات

النقدية , والوفاء بقيمة الفواتير , وإجراء كافة الخدمات الاستعلامية , وأجراء الحوالات بين حساباته داخل البنك , أو مع جهات خارجية .

إن غالبية البنوك في العالم قد أنشأت بشكل أو بآخر مواقع معلوماتية تعد من قبيل المواد الدعائية ، واتجهت معظم المواقع إلى استخدام بعض وسائل الاتصال التفاعلي مع العميل ، على عكس المواقع التبادلية ، التي لا تزال اتجاهات البنوك نحوها تخضع لاعتبارات عديدة ، فهذه المواقع تعني قدرة العميل على التعامل مع الخدمة المصرفية عن بعد ومن خلال الانترنت .

ومن أهم هذه الخدمات التي تقدمها المصارف الإلكترونية:

- تقديم الاستعلامات اللازمة للعملاء .
- إتمام عمليات التحويل بين الحسابات الداخلية ومع بنوك وشركات أخرى .
- الحصول على كشوف الحسابات أو غيرها من التقارير التي يحتاجها العميل .
- سداد الأقساط المستحقة أو الفواتير الدورية .
- تقديم الطلبات الشخصية قبل الحضور إلى البنك مثل طلبات الحصول على بطاقات ائتمانية .

3. بيئة المصارف الالكترونية وتأثيرها على عمل هذه البنوك :

من فترة قصيرة مضت لم نكن نسمع أحدا يقر بأن شبكة الإنترنت بيئة آمنة، وربما لا يزال الوضع كذلك، إن تحقيق درجة مقبولة من الأمن على الشبكة أمسى أهم متطلبات القيام بأعمالها ، وتصبح مشكلة امن المعلومات أكثر حدة بالنسبة لعمليات التحويل النقدي بأشكالها المختلفة . غير أن الاتجاه نحو قبول الانترنت كواسطة تبادل يزداد يوما بعد يوم، ربما بسبب شيوع الاهتمام بأمنها ، وتحديداً عبر الإبداع المتزايد في ميدان وسائل امن التقنية وامن المعلومات، إلى جانب الاهتمام التشريعي والتنظيمي لتوفير الحماية لبيانات ومعلومات الانترنت ، وربما ، بسبب إن البنوك الفاعلة الكبرى دخلت المعركة وشيئا فشيئا تضيق فرص الاختيار بين العمل على الشبكة أو البقاء خارجها ، وتتجه عوامل السوق واستراتيجيات التسويق والإدارة نحو استثمار الانترنت بيئة للعمل ، لأنها تحتل مكانا يتسع يوما بعد يوم في ميدان النشاط التجاري والمالي .

إن المستخدمين تتزايد قناعتهم بتحقق مستوى من الأمن ، لكن خياراتهم تتوقف على مدى فعالية إجراءات الأمن ، ومن هنا كان التحدي الأول لصناع القرار هو امن المعلومات وتحصين مواقع العمل من الاختراقات الخارجية والداخلية ، ولعل من أكثر العوامل مساهمة في الاتجاه نحو قبول التعامل المالي على الشبكة نشوء ووجود بوالص تامين على مخاطر العمل عبر الشبكة ، حيث انه بقدر توفر التأمين من الخطر تتلاشى الخشية

من حصوله ، لان المال مضمون ، إن لم يكن بسبب ما تفرضه وتتطلبه شركات التامين من إجراءات سلامة وامن ، فبفضل وجود التعويض عند تحقق الخطر[4] .

4. أهمية البنوك الالكترونية :

إن العميل بحاجة للحصول على حل لمشكلته وليس مشاهدة عرض يقدم له، هذه أول الحقائق التي يمثل إدراكها مبرر وجود البنك الالكتروني بل أساس نجاحه ، لهذا , كان موقع شركة E-Loan المتخصصة بالإقراض الالكتروني – على سبيل المثال – مميزاً بين سائر المواقع الشبيهة ويميزها عن جهات الإقراض غير الالكترونية، لأنه ليس مجرد موقع يعرض الإقراض بالوسائل التقنية ، بل لأنه يساعد المستخدمين على تحديد وحساب احتياجاتهم , وخياراتهم المتطلبة لحل مشاكلهم , ثم يقدم حزمة من العروض والخدمات التي تتفق مع رغبة وطلب العميل .

إن البنوك غير الالكترونية ، تقدم جزءا من الحلول لمشكلات العميل لكنها لا تقدم حلولا شاملة , أو تقدم حلولا جزئية بكلف عالية ، فإذا علمنا إن التنافس على أشده في سوق العمل المصرفي ، وعنوانه الخدمة الشاملة والأسرع بالكلفة الأقل ، فان البنوك الالكترونية فرصة لتحقيق معدلات أفضل للمنافسة والبقاء في السوق ، وببساطة ، فان الظن ان البنك الالكتروني مجرد إدارة لعمليات مصرفية وحسابات مالية ظن خاطئ ، لان التقنية تتيح للعميل ذاته أن يدير مثل هذه الأعمال ، أن وجود البنك الالكتروني مرهون بقدرته على التحول إلى موقع للمعلومة ومكان للحل المبني على المعلومة الصحيحة ، انه مؤسسة للمشورة ، ولفتح آفاق العمل ، انه مكان لفرص الاستثمار وإدارتها ، مكان للخدمة المالية السريعة بأقل الكلف، مكان للإدارة المتميزة لاحتياجات العميل مهما اختلفت ،

كموقع Intuit Quicken. Com إذ يلحظ المستخدم ان هذا الموقع يقدم خدمات مالية وضريبية واستشارية واستثمارية ويعرض حزما من الخدمات الشاملة تتلاقى مع متطلبات الزبائن لحل مشكلاتهم .

كما أن الاتجاه نحو الدفع النقدي الالكتروني المصاحب لمواقع التجارة والأعمال الالكترونية يقدم مبررا لبناء البنوك الالكترونية ، فشركات التامين , النفط ، الطيران ، الفنادق ، ...الخ تتجه بخطى واثقة نحو عمليات الدفع عبر الخط , أو الدفع الالكتروني ، وهي عمليات تستلزم – إن لم يكن موقع الشركة يوفر وسائل الدفع النقدي – وجود حسابات بنكية أو حسابات تحويل أو نحوها ، وترك الساحة دون تواجد يعني دفع القطاعات المشار إليها إلى ممارسة أعمال مالية على الخط لسد احتياجاتها التي لا توفرها جهات العمل المصرفي المتخصصة .

إن البنوك الالكترونية توفر في التكاليف، حيث إنها تحتاج إلى عدد اقل من الموظفين كما إنها توفر في تكاليف الوجود المادي، إن هذا الوفر ليس بالضرورة إن تعود للبنك نفسه , و إنما قد تستخدم في تقديم الخدمات بأسعار أقل .

5. مزايا ومخاطر المصارف الإلكترونية:

تتمثل مزايا المصارف الألكترونية في[5]:

- تنظيم عمليات الدفع الدوري: يعنى الاتفاق على وقت محدد لاستقطاع جزء محدد من الرصيد وتحويله إلى المستفيد بشكل دوري ومن دون أخطاء .
- السلامة والأمن: كان للتحويلات الالكترونية دور كبير في إزالة المخاوف من عمليات السرقة للنقود أو للشيكات .
- تحسين عمليات التدفق النقدي: وهي سرعة تنقل النقد بشكل كبير وبثقة عالية .
- تقليل الاعتماد على الأعمال الورقية: وذلك لندرة احتياج الأعمال المصرفية للنماذج الورقية .
- زيادة رضا العملاء من خلال سرعة ودقة إنجاز معاملتهم .

أما مخاطر البنوك الإلكترونية فتتمثل في:

لا أحد يستطيع إنكار الكم الهائل من المزايا التي تقدمها البنوك الالكترونية، إلا أن ذلك لا يعني التعامل من خلال البنوك الالكترونية ليس له مخاطر وعيوب حيث نجد الخبراء الاقتصاديين يحذرون من عيوب محتملة الحدوث من نظام التعامل مع البنوك الالكترونية ومنها :

ظهور فجوة في علاقة البنك بالعميل يمكن أن تتسبب في عمليات نصب تتعرض لها البنوك .

صعوبة السيطرة على حجم السيولة في البنوك وذلك لأن العملاء يستطيعون تحويل أي مبلغ من خلال الكمبيوتر ومن دول أخرى , مما يؤثرتأثيرا سلبياً على اقتصاديات الدول أو التسبب في أزمات سيولة .

المحور الثاني: أمن المعاملات والمعلومات المصرفية الإلكترونية

تشكل المعلومات المصدر الأساسي الذي يتيح للمصارف اتخاذ القرارات المناسبة ويمكنها من تأدية مهامها، إذ أن نوع المعلومات وكميتها وطريقة عرضها تعتبر الأساس في نجاح عملية صنع القرارات داخل أي مؤسسة معاصرة، وعليه فإن للمعلومات قيمة عالية تستوجب وضع الضوابط اللازمة لاستخدامها وتداولها ووضع السبل الكفيلة بحيازتها، لذا فإن المشكلة التي يجب أخذها بالحسبان هو توفير الحماية اللازمة للمعلومات وإبعادها عن الاستخدام غير المشروع لها.

1. تعريف أمن المعلومات :

من ضمن المفاهيم التي أعطيت لأمن المعلومات نجد:

- "هو مجموعة من الإجراءات والتدابير الوقائية التي تستخدم سواء في المجال التقني أو الوقائي للحفاظ على المعلومات والأجهزة والبرمجيات إضافة إلى الإجراءات المتعلقة بالحفاظ على العاملين في هذا المجال"[6]؛
- والبعض عرفه بأنه: "الحفاظ على المعلومات المتواجدة في أي نظام معلوماتي من مخاطر الضياع والتلف أو من مخاطر الاستخدام غير الصحيح سواء المتعمد أو العفوي أو من مخاطر الكوارث الطبيعية"؛
- ويعرف أيضا: "هو العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها، ومن زاوية تقنية، ومن زاوية قانونية، فإن أمن المعلومات هو محل دراسات وتدابير حماية وسرية وسلامة محتوى المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة"[7].

ومن خلال كل ماسبق يمكن أن نعرف أمن المعلومات بأنه" **ذلك الحقل الذي يهتم بدراسة طرق حماية البيانات المخزنة في أجهزة الحواسيب والأجهزة الملحقة وشبكات الاتصالات والتصدي للمحاولات الرامية إلى الدخول غير المشروع إلى قواعد البيانات المخزنة أو تلك التي ترمي إلى نقل أو تغيير أو تخريب تلك المعلومات**".

2. عناصر أمن المعلومات:

إن الغرض من وسائل أمن المعلومات سواء من الناحية التقنية أو الأدائية هو ضمان توفر العناصر التالية لأية معلومة يراد توفير الحماية الكافية لها[8]:

- ✓ **السرية والموثوقية:** وتعني التأكد من أن المعلومات لا تكشف ولا يطلع عليها من قبل الأشخاص غير المخولين بذلك؛
- ✓ **التكاملية وسلامة المحتوى:** التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله أو العبث به وبشكل خاص لن يتم تدمير المحتوى أو تغييره أو العبث به وبشكل خاص لن يتم تدمير المحتوى أو تغييره في أي مرحلة من مراحل المعالجة أو التبادل سواء في مرحلة التعامل الداخلي مع المعلومات أو عن طريق تدخل غير مشروع؛
- ✓ **استمرارية توفر المعلومات:** التأكد من استمرار عمل النظام المعلوماتي واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة لمواقع المعلوماتية، وأن مستخدم المعلومات لن يتعرض إلى منع استخدامه لها أو دخوله إليها؛
- ✓ **عدم انكار التصرف المرتبط بالمعلومات ممن قام به:** ويقصد به ضمان عدم إنكار الشخص الذي قام بتصرف ما متصل بالمعلومات أو مواقعها إنكار أنه هو الذي قام بهذا التصرف، بحيث تتوفر قدرة إثبات أن تصرفا ما قد تم من شخص ما في وقت معين.

وتطالب كل من منظمة التعاون والتنمية الاقتصادية والاتحاد الأوروبي في العديد من التقارير المتعلقة بالإدارة الإلكترونية ضرورة الإلتزام بأربعة وظائف أو مستويات أساسية لضمان تأمين أنظمة المعلومات والإدارة الإلكترونية وهي:

- **الخصوصية:** ويقصد بها أن الولوج إلى المعلومات المتاحة في شكل إلكتروني تقتصر فقط على الأطراف المشاركة في الاتصال(الأشخاص، التطبيقات، البرمجيات، والأجهزة)، وتستند الخصوصية على مبدأ التشفير الذي يمكن إجراءه على البيانات والمعلومات؛
- **وحدة البيانات واستقامتها:** يؤدي الالتزام بوحدة البيانات واستقامتها إلى ضمان أن المعلومات المتبادلة لم يتم التدخل فيها أو تعديلها وذلك في الفترة مابين إرسالها من جانب المرسل واستقبالها بواسطة المرسل إليه، فبدون الاستناد إلى تطبيقات التوقيع الإلكتروني، من العسير اكتشاف أي تعديلات أو تغييرات تطرأ على مستند أو نص معين؛
- **عدم التنصل(عدم القدرة على الإنكار):** أي لايمكن لأي طرف من الأطراف المشاركة في عملية التراسل إنكار القيامة بالمعاملة، ولضمان عدم النكران لابد أن تتوافر إمكانية التتبع المستمر للمعاملة التي

يتم القيام بها، وبالتالي معارضة أي رفض لها من خلال الإثبات الحاسم بالقيام بها، ويتعلق هذا الأمر باستخدام مجموعة متنوعة من آليات التوقيع الإلكتروني منها منظومة تأكيد الإرسال والاستقبال والاستناد إلى تقنية تعمل على ضمان الحصول على تاريخ ووقت إجراء المعاملة، وهذه التقنية يطلق عليها العمل على أرشفة المعاملة والتوقيع المرتبط بها؛

- **التحقق والتعرف على المستخدم:** يكمن الهدف من وراء التحقق أو التوثيق التأكد من أن هوية المستخدم سواء كانت(اسم مستعار، أو حقيقي، أو عنوان.....) تكون هوية متعارف عليها؛

3. المخاطر التي تواجه أمن المعلومات :

لقد أصبح اختراق أنظمة المعلومات ونظم الشبكات والمواقع المعلوماتية خطرا يقلق العديد من المصارف في السنوات الأخيرة ومع مرور الزمن نجد أنه على الرغم من سبل الحماية التي تتبعها المصارف، إلا أن هناك ارتفاعا واضحا في معدل الاختراقات مع تنوع الوسائل المستخدمة في الاختراق، أما عن طبيعة الأخطار التي يمكن أن تواجهها نظم المعلومات فهي عديدة، فالبعض منها قد يكون مقصود كسرقة المعلومات أو إدخال الفيروسات، وغيرها وهي الأشد ضررا على نظم المعلومات ويكون مصدرها أحيانا من داخل أو خارج المصرف، أما البعض الآخر فقد يكون غير مقصود كالأخطاء البشرية والكوارث الطبيعية ويمكن تصنيف الأخطار المحتملة التي يمكن أن تتعرض لها نظم المعلومات إلى ثلاث فئات[9]:

- **الأخطاء البشرية** : هي التي يمكن أن تحدث أثناء تصميم التجهيزات أو نظم المعلومات أو خلال عملية البرمجة أو تجميع البيانات أو أثناء إدخالها إلى النظام، أو في عمليات تحديد الصلاحيات للمستخدمين، وتشكل هذه الأخطاء الغالبية العظمى للمشاكل المتعلقة بأمن وسلامة نظم المعلومات في المصرف؛
- **الأخطار البيئية:** وتشمل الزلازل والعواصف والفيضانات والأعاصير والمشاكل المتعلقة بأعطاب التيار الكهربائي والحرائق.....التي تؤدي بدورها إلى تعطل عمل التجهيزات وتوقفها لفترات طويلة نسبيا لإجراء الإصلاحات اللازمة واسترداد البرمجيات وقواعد البيانات؛
- **الجرائم المحوسبة:** تمثل تحديا كبيرا لإدارة نظم المعلومات لما تسببه من خسارة كبيرة ويتم التمييز بين ثلاث مستويات للجرائم المحوسبة وهي: سوء الاستخدام المقصود لجهاز الحاسوب ، سوء الاستخدام لجهاز الحاسوب بشكل غير قانوني، اختراق نظام الحواسيب من قبل أشخاص داخل المصرف أو خارجه.

4. الحماية من أخطار أمن المعلومات :

تعتبر عملية الحماية من الأخطار التي تهدد أنظمة المعلومات من المهام المعقدة والصعبة والتي تتطلب من إدارة نظم المعلومات الكثير من الوقت والجهد والموارد المالية وذلك للأسباب التالية:

- العدد الكبير من الأخطار التي تهدد عمل نظم المعلومات؛
- توزع الموارد المحوسبة على العديد من المواقع التي يمكن أن تكون أيضا متباعدة؛
- صعوبة الحماية من الأخطار الناتجة عن ارتباط المصرف بالشبكات الخارجية؛
- التقدم التقني السريع يجعل الكثير من وسائل الحماية متقادمة من بعد فترة وجيزة من استخدامها؛
- التأخر في اكتشاف الجرائم المحوسبة مما لا يتيح للمصرف إمكانية التعلم من التجربة والخبرة المتاحة؛
- تكاليف الحماية يمكن أن تكون عالية لا يمكن تحملها.

وتقع مسؤولية وضع خطة الحماية للأنشطة الرئيسية على مدير نظم المعلومات على أن تتضمن هذه الخطة إدخال وسائل الرقابة التي تضمن تحقيق مايلي:

- الرقابة من الأخطار غير المعتمدة؛
- إعاقة أو صنع الأعمال التخريبية المتعمدة؛
- اكتشاف المشاكل بشكل مبكر قدر الإمكان؛
- المساعدة في تصحيح الأعطاب واسترجاع النظام.

ويمكن تصميم نظام الرقابة ضمن عملية تطوير نظام المعلومات ويجب أن يركز هذا النظام على مفهوم الوقاية من الأخطار، ويمكن أن يصمم لحماية جميع مكونات النظام بما فيها التجهيزات والبرمجيات والشبكات[10].

المحور الثالث: أمن المعلومات ودوره في تفعيل نشاط الصيرفة الإلكترونية

هناك علاقة تكاملية بين أمن المعلومات ونشاط الصيرفة الإلكترونية، حيث كلما كان أمن المعلومات متوفر كلما كان نشاط الصيرفة أكثر فعالية، لماذا؟

لأن أمن المعلومات سيضمن السرية والسرعة التي تعتبر من ضمن المبادئ الهامة التي تلتزم البنوك بها في أداء وظائفها وتنمية معاملاتها.

وتشير حصيلة دراسات أمن المعلومات وما شهده هذا الحقل من تطورات على مدى الثلاثين عاما المنصرمة أن مستويات ومتطلبات الأمن الرئيسية في بيئة تقنية المعلومات تتمثل في الوعي بمسائل الأمن لكافة مستويات الأداء الوظيفي من خلال الحماية المادية للتجهيزات التقنية والحماية الأدائية (استراتيجيات رقابة العمل والموظفين)، وهي الحماية التقنية الداخلية والحماية التقنية من المخاطر الخارجية[11].

كما أنه لا يمكن أن تتكامل حلقات الحماية دون الحماية القانونية من خلال النصوص التشريعية التي تحمي البنوك الإلكترونية من إساءة استخدام الحواسيب والشبكات أو ما يصطلح عليه بجرائم الكمبيوتر والانترنت والجرائم المالية الإلكترونية.

وإذا أردنا الوقوف في حدود مساحة العرض المتاحة على ملخص الاتجاهات الأمنية في حقل حماية البيانات في البيئة المصرفية والتي تتخذ أهمية بالغة بالنسبة للبنوك التي تمثل بياناتها في الحقيقة أموالا رقمية وتمثل حقوقا مالية وعناصر رئيسية في الائتمان، نجد أن المطلوب هو وضع إستراتيجية شاملة لأمن المعلومات تتناول نظام المصرف وموقعه الافتراضي، وتتناول الحماية الداخلية من أنشطة إساءة الاستخدام التي قد يمارسها الموظفون المعنيون داخل المنشأة وتحديدا الجهات المعنية بالوصول إلى نظم التحكم والمعالجة والمبرمجين، إلى جانب إستراتيجية الحماية من الاختراقات الداخلية، وهذه الاستراتيجيات يجب أن تمتد إلى عميل المصرف لا للبنك وحده، حتى نضمن نشاطا واعيا للتعامل مع المعلومات وتقدير أهمية حمايتها، ولكل إستراتيجية أركانها ومتطلباتها ومخرجاتها، وتقييم كفاءة الإستراتيجية يقوم على مدى قدرتها على توفير مظلة أمن شاملة لنظام المصرف والعميل والنظم المرتبطة بهما.

الخاتمة :

تعتبر البنوك الإلكترونية بمثابة تحد جديد أما المصارف بالنظر إلى المشاكل التي أصبحت تعترض القطاع المصرفي خاصة تلك المتعلقة بجودة المعلومة والحفاظ على سريتها وأمنها لذلك يعتبر تطوير وسائل الحماية المعلوماتية أمر له أهمية بالغة في تفعيل نشاط الصيرفة الإلكترونية، فمن خلال أمن المعلومات فإن الخدمة المصرفية سوف تتمتع بجميع خصائص جودتها وعلى رأسها السرية والخصوصية والموثوقية التي توفر خدمة مصرفية بكافة المقاييس، كل هذا من شأنه أن يزيد من ثقة الزبون بالخدمات المصرفية الإلكترونية لظروف الراحة والأمان التي يشعر بها، ومن هنا نستنتج أن أمن المعلومات لايلعب دورا فقط في جودة الخدمات المصرفية الإلكترونية ولكنه هو أساس وجودة الخدمة المصرفية.

- **النتائج**: من خلال الدراسة توصلنا إلى النتائج التالية:

✓ أمن المعلومات هو الحقل الذي يدرس طرق حماية البيانات المخزنة في أجهزة الحاسوب إضافة إلى الأجهزة الملحقة وشبكات الاتصالات والتصدي للمحاولات الرامية إلى الدخول غير المشروع في قواعد البيانات المخزنة أو تلك الرامية إلى نقل أو تغيير أو تخريب القواعد المعلوماتية؛

✓ من ضمن عوائق الصيرفة الإلكترونية هو غياب النصوص القانونية التي تقوم بردع الجرائم الإلكترونية.

- **التوصيات** : بناء على ماسبق نقدم التوصيات التالية :

✓ توعية عملاء البنوك بعمليات الاحتيال والنصب المالي والمصرفي الإلكتروني وبعمليات الاحتيال التي تتعرض لها البطاقات المصرفية ؛

✓ المراجعة الدورية للتدقيق في شخصية وسلوك الأفراد العاملين من وقت لآخر وربما يتم تغيير مواقع عملهم ومحاولة عدم احتكار المهام على موظفين محددين؛

✓ ضرورة قيام الدولة بوضع قوانين وتشريعات شاملة فيما يخص التعامل بشبكة الويب، وتحمل عقوبات لجرائم الانترنت خصوصا المتعلقة بالعمل المصرفي؛

✓ ضرورة قيام الدولة بوضع قوانين وتشريعات شاملة تحكم التعامل بالصيرفة الإلكترونية، تحدد فيها مسؤوليات وواجبات كل من المصرف والعميل.

الهوامش والإحالات :

[1] نور الدين جليد، أمينة بركان، **الصيرفة الإلكترونية والمصارف الإلكترونية**، مجلة العلوم القانونية والاقتصادية، العدد العاشر، جوان 2011، ص 253.

[2] نصر حمود مزنان فهد، **إمكانات التحول نحو الصيرفة الإلكترونية في البلدان العربية**، مجلة كلية الإدارة والاقتصاد، العدد 04، 2011، ص ص 04-03.

[3] حسن يوسف، **البنوك الإلكترونية**، الطبعة الأولى، دار الصفاء القانونية، القاهرة، مصر، 2012، ص 57.

[4] هند خليفة، **البنوك الإلكترونية وخدماتها على الإنترنت**،جريدة الرياض ، 04 جانفي 2005، العدد13343 ، ص 213.

[5] حسن يوسف، مرجع سابق، ص 62.

[6] زيدان مُحَّد، مُحَّد جمو، **متطلبات أمن المعلومات المصرفية في بيئة الانترنت**، المؤتمر السادس لجمعية الكتبات والمعلومات السعودية "بيئة المعلومات الآمنة: المفاهيم والتشريعات والتطبيقات"، المنعقد بمدينة الرياض، خلال الفترة 06-07 أفريل 2010.

[7] منصور بن سعيد القحطاني، **مهددات الأمن المعلوماتي وسبل مواجهتها**، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، 2008، ص 30.

[8] عدمان مريزق، بوقلاشي عماد، **الأمن المعلوماتي في ظل التجارة الإلكترونية–إشارة إلى حالتي الجزائر وتونس–**، مداخلة مقدمة ضمن الملتقى العلمي الدولي الرابع حول: عصرنة نظام الدفع في البنوك الجزائرية وإشكالية اعتماد التجارة الإلكترونية في الجزائر–عرض تجارب دولية–، جامعة سطيف، ص05

[9]منصور بن سعيد القحطاني، مرجع سابق، ص33.

[10] عطا الله أحمد الحسبان، **مدى تعامل مدققي أنظمة تكنولوجيا المعلومات بمعايير التدقيق الدولية الخاصة ببيئة أنظمة المعلومات للمحافظة على أمن وسرية المعلومات في البنوك التجارية الأردنية**، مجلة أربد الأهلية، الأردن، 2012، ص 362.

[11] خبابة عبد الله، **الاقتصاد المصرفي**، مؤسسة شباب الجامعة، الاسكندرية، مصر، 2008، ص ص 115–116.