محددات ومتطلبات حماية الأنظمة المعلوماتية في المصرف

Determinants and requirements of the protection of information systems in the bank

د. عبدالهادي مسعودي[1] د. خيـرة مسعـــودي[2]

1 أستاذ محاضر أ - جامعة الأغواط- الجزائر.Abdelhadi.messe@yahoo.fr

[2]أستاذة مؤقتة – جامعة الأغواط- الجزائر.,messkhei@gmail.com

تاريخ الاستلام: 2018/07/23 تاريخ القبول: 2019/01/21 تاريخ النشر: 2019/02/01

مستخلص:

تعالج هذه الورقة بعض مشاكل التطور الذي أحدثته الثورة المعلوماتية وتطبيقاتها المعقدة، هذا التطور الذي نمت معه وتعددت أساليب جديدة من الجرائم اتخذت مظاهر مختلفة والتي أصبحت تطرح إشكاليات عديدة وتشكل خطرا على التوظيفات والاستثمارات البنكية والمالية، ويستمد هذا البحث أهميته من خلال توضيح سبل الحماية والأمان أمام التهديدات المختلفة وفهم عمل تلك الأنظمة من أجل سلامة وأمن المعلومات وخصوصية الزبائن وتنمية التعاملات المصرفية الالكترونية بأكثر راحة واطمئنان.

الكلمات المفتاحية: حماية، أمان، أنظمة أمنية، أمنية المعلومات، أمنية الشبكات.

Abstract:

This paper addresses some problems of the development which caused the revolution IT and applications of the complex, a development that has grown with him and numerous new methods of crime has taken different aspects that have become problematic are numerous and pose a threat to investments and investment banking, financial, and draws this research significance by clarifying the ways of protection and security to the different threats and understand the work of those regulations for the safety and information security and privacy of customers and the development of electronic banking transactions more convenient and reassuring.

Key words: Protection - Security - Security Systems - information security - network security.

Jel Classification Codes: E59, G22, O14

الاستاذ المرسل: د. عبدالهادي مسعودي، **Abdelhadi.messe@yahoo.fr**

مقدمة:

يعد التعامل الالكتروني من نتائج التعامل المصرفي، فمع تطور التكنولوجيات وازدياد التعامل بأسلوب التجارة الالكترونية. ظهرت أساليب مبتكرة لسداد المدفوعات، كالبطاقات الالكترونية والأوراق التجارية الالكترونية والنقود الالكترونية... الخ؛ ومع أن تنفيذ نظم الدفع الالكترونية لا تزال في بداية الطريق وهي تحت تطور المقومات الفنية والاقتصادية والثقافية والقانونية لنظم الدفع الالكتروني، وهناك عدد من المقترحات والتطبيقات التنافسية تظهر في التعاملات الالكترونية لتسوية المعاملات وأمنها.

ويتسم العصر الحالي ببروز تكنولوجيا الخيارات النقدية الالكترونية سواء من حيث المصدر أو من حيث التقنية أو عن طريق التسوية أو الخدمات الممنوحة...؛ وعلى أية حال يعتبر موضوع أدوات الدفع الالكترونية بلا أدنى شك من الموضوعات النقدية الأكثر صعوبة والأكثر إثارة لاهتمام الأطراف الاقتصادية والسلطات النقدية في الاقتصاد الحديث، وتكتسب تلك الأهمية في العالم النامي أهمية خاصة من واقع ما يفرضه العالم المعاصر من حتمية تطوير وسائل الدفع لمواجهة انتشار وسائل الدفع الأجنبية والعالمية وتوفير وسائل تتطلب تغطية المعاملات الأوتوماتيكية عن بعد كالأنترنت وما شابه.

وعلى وجه الإجمال يمكن اعتبار نظم الدفع الالكترونية أحد الظواهر التجارية النقدية المتطورة بالنظر إلى ما أفضت إليه من تعديل عميق في تنظيم الأسواق والتوزيع والتبادل الالكتروني، حيث تقدم إمكانيات وآفاق جديدة للاتصال بالزبائن والتجار والبنوك على حد سواء، نظرا لتفاديها المشكلات الأساسية للتعامل بالنقود السائلة (العد، التخزين، النقل، الإيداع، السحب..) بالإضافة إلى المزايا التي تتمتع بها كتقليل الحجم النقدي المستخدم وتخفيض تكلفة المعاملات ومجانيتها في بعض الحالات وانتشارها في جل الأماكن وفي اغلب الأوقات؛ ولكن مع تلاحق التطورات التكنولوجية وتباين استخداماتها في المجتمعات المتقدمة وغيرها من الدول، ظهرت هناك العديد من المخاوف المثارة حول نظم الدفع الالكترونية والتوسع مستقبلا لتعاملاتها ومدى تأثير ذلك على الأوضاع الاقتصادية للدول وقدرة الحكومات بالسيطرة على نشاطات الشركات المصدرة والراعية لبرامج الدفع الالكترونية؛

وعلى اعتبار أن تطبيقات العمل المصرفي الالكتروني تزداد يوما بعد يوم دقة وتعقيدا في مكوناتها واستعمالاتها وتتوسع في غير اتجاه لتأدية أكبر عدد من الخدمات في ظل سوق مفتوحة على تنافس حاد في كل المستويات الأمر الذي أدى إلى رواج الخدمات المصرفية الالكترونية وسط تعاظم الاعتماد على الشبكات المفتوحة على التقنيات المتطورة على نحو واسع. وبهذه التطورات وانتشار هذه

التطبيقات أضحى من الواجب على المصارف وضع استراتيجية لحماية التكنولوجيات البنكية والأنظمة المعلوماتية في المصرف حتى يتم تفعيل العمل المصرفي إلى أبعد الحدود.

ومن هذا المنطلق تأتي هذه الدراسة لتشير بوضوح إلى محاولة الفهم الصحيح لتطبيقات نظم الدفع الالكتروني وآثارها، وحاجة البنوك إلى تأسيس نظام أفضل للاستغلال الأعظم للمزايا التي تقدمها نظم الدفع الالكترونية وتفادي الأخطاء والعيوب في مجال التقنية البنكية المتاحة؛ حيث سنحاول الإشارة إلى محددات وآثار استخدام نظم الدفع الالكترونية الحديثة في تحسين الخدمة المصرفية وتحديد متطلبات العمل المصرفي في بيئة الأعمال الالكترونية وطرق حمايتها، من خلال مناقشة الإشكالية التالية: **مـاهي محددات ومتطلبات حماية الأنظمة المعلوماتية في المصرف.**

00000

I. مدخل لأنظمة الدفع الالكترونية: تسعى البنوك جاهدة إلى تطوير نظم الدفع الالكترونية من خلال البطاقات البنكية المنتشرة والنظم النقدية الالكترونية المختلفة وأجهزة الصرف الآلية الموزعة عبر نقاط متعددة، وانتشرت هذه الخدمات بصورة متزايدة ورهيبة وانفتحت على شبكة الانترنت وقنوات الاتصال الأخرى. ويعالج هذا الجانب مدخل لنظم الدفع الالكترونية على النحو الاتي:

1. **تعريف أنظمة الدفع الالكترونية:** تعني أنظمة الدفع الالكترونية استخدام أجهزة الحواسيب أو شبكة الانترنت وتقنيات الاتصال الحديثة كوسائل جوهرية في تنفيذ عمليات الدفع وتسوية المعاملات المالية الكترونيا، وهناك طرق وأساليب متعددة للتطبيقات التقنية في أنظمة الدفع؛ فمنها ما يعتمد على تقنية البطاقة البنكية، ومنها ما يعتمد على تقنية الاتصال مثل الشبكات واستعمالات النقود الالكترونية، ومنها ما يعتمد على أنظمة الذكاء[1]، كما تعرف أنظمة الدفع بأنها كل عملية تحويل أموال بموجب شيك أو سند أو أي أوراق أخرى والتي تنفذ بواسطة نقطة الكترونية عبر أية وسيلة اتصال، ويقصد بالنقطة الالكترونية الجهاز الذي يسمح بإنشاء عملية تحويل أموال الكترونيا[2].

وهي عبارة عن نظم قائمة بذاتها من خلال مواقع الكترونية تقدم خدمات مصرفية ومالية وتجارية وإدارية شاملة، لها وجود مستقل على الشبكة الالكترونية قادرة على التعاقد وتقديم الخدمات المصرفية[3]؛ أو هي النظام الذي يتيح للزبون الوصول إلى حساباته أو أية معلومات يريدها، والحصول على مختلف الخدمات والمنتجات المصرفية من خلال شبكة المعلومات التي يرتبط بها جهاز الكمبيوتر الخاص به أو الوسائل الالكترونية أو الرقمية أو الآلية الأخرى[4].

2. **قنوات أنظمة الدفع الالكترونية:** تتيح هذه القنوات إجراء العمليات المصرفية من خلال أجهزة وبطاقات الكترونية يتم التعامل بها بواسطة أنظمة دفع وتحويل، والتي تم تحديد أشكالها في الأنماط التالية:

1.2. البطاقة البنكية: تمثل هذه البطاقات أهم وسائل الدفع الالكترونية التي انتشرت على مستوى العالم انتشارا واسعا حيث يتعامل بها الملايين من الأفراد، وأطلق على هذه الوسيلة في التعامل المالي والاستعمال المصرفي عدة أسماء منها بطاقة الائتمان، بطاقة الاعتماد، بطاقة الدفع الالكترونية، بطاقة الوفاء أو البطاقة البلاستيكية[5].

وتعرف البطاقة بأنها نظام تعاقدي متميز مستقل بعناصر، جوهره فكرة الإقراض بفائدة، تتضمن بيانات رقمية تحدد الجهة المصدرة لها وهوية الشخص الحامل لها ونطاق صلاحيتها[6]. أو هي أداة مصرفية بلاستيكية كبديل للنقد والوفاء والائتمان تعطي لحاملها الحق في الحصول على تسهيل ائتماني من مصدر البطاقة[7]. كما تعرف بأنها النظام الذي يستند إلى قيام جهة معينة " في الغالب بنك " بإصدار بطاقة من البلاستيك أو من أي مادة تضمن المتانة والسلامة وعدم التلف أو إمكانية التزوير لصالح شخص آخر[8].

2.2. أجهزة الصراف الآلي[9] ATM: الصراف الآلي الذي يعرف اختصارا بـ **ATM** أو آلة المال أو البنك آلة أو نقطة السحب وهي عبارة عن أجهزة مبرمجة تحفظ فيه النقود بطريقة معينة تستطيع التعرف على بطاقة الزبون وتحدد العملية التي يريدها، وبسعة محدد من العملات، وتعد للحالات الطارئة للزبون حفاظا على وقته وتسهيلا لحاجاته وهو محدودة من حيث عدد مرات وكمية النقود، وتعرف بأنها هي تلك الآلات التي يمكن نشرها بالأماكن المختلفة سواء بالجدار أو بشكل مستقل، وتكون متصلة بشبكة حاسوب البنك، وبواسطة بطاقة بلاستيكية أو بطاقة ذكية، يمكن للزبون الحصول على الخدمات المختلفة كالسحب النقدي والإيداع والاستفسار عن الحساب ..الخ[10]. أو هي جهاز إخطار مؤتمم لتوفير خدمة السحب النقدي في أماكن مختلفة دون الرجوع للبنك وفي كل الأوقات[11].

3.2. النقود الالكترونية: هناك عدة مصطلحات للتعبير عن مفهوم النقود الالكترونية فقد يطلق عليها النقود الرقمية ***Digital Money*** أو العملة الرقمية ***Digital Currency*** وقد يطلق عليها النقدية الالكترونية **e-*cash*** وهي مجرد بتات ***bits*** يمكن حفظها على القرص الصلب للحاسوب أو في ذاكرة المساعد الرقمي أو البطاقة الذكية ***smart card***[12]؛ بينما **عرفها بنك التسويات الدولية**: بأنها قيمة نقدية في شكل وحدات ائتمانية مخزنة بشكل الكتروني أو محمولة على أداة الكترونية يحوزها المستهلك[13]. في حين **عرف الإرشاد الأوربي رقم 46 سنة 2000** النقد الالكتروني بأنه قيمة نقدية

مخلوقة من المصدر تحتوي على خصائص معينة كالتخزين على الوسط الالكتروني والإيداع المالي والقبول[14].

II. أشكال أنظمة الدفع الالكترونية: تتعدد أشكال نظم الدفع الالكترونية في التعاملات المصرفية، أين تسارعت مختلف الشركات العالمية في مجال التكنولوجيا البنكية بطرح عدة منتجات بنكية تحددت أشكالها في النظم التالية:

1. **نظم النقود الالكترونية:** يتم إصدار النقود الالكترونية في ثلاث نظم متميزة وهي:

1.1. **نظام الـ *Cyber Cash*:** يتميز هذا النظام بارتباطه بنظام مركزي يعطي وحدة النقد قيمتها دون أن تكون متضمنة فيها وبالتالي لا تخزن في الذاكرة بل تحول كأمانة إلى محفظة مركزية للنظام ***Cyber Cash Wallet*** موجودة في ***Cyber Cash Bank*** ولا يحتاج الزبون لحساب لدى البنك بل يتم تحويل قيمة المعاملات من محفظته إلى سجل التاجر الرقمي، وهكذا يعطي نموذج ***Cyber Cash*** عملية مركزية لإتمام المعاملات من خلال الاحتفاظ بسير النقود المحولة[15].

2.1. **نظام الـ *Digi Cash*:** صمم نظام ***e-cash*** كأداة دفع مضمونة تنتقل من حاسوب لأخر عبر البريد الالكتروني أو الانترنت فمن يحوز ***e-cash*** يحوز قيمة النقود، ويمكن عرض طرقة عمل النظام وفق المراحل التالية التي لا تستغرق سوى ثوان معدودة[16]:

- يتصل الزبون بالبنك (مؤسسة الإصدار) ويسحب منه وحدات **e-*cash*** من فئات وقيم مختلفة؛
- يتم إيداع قيمة النقود رقميا في ذاكرة الحاسوب " المحفظة الالكترونية" ويتم تشفير قيمة تلك الوحدات التي تأخذ رقما متسلسلا خاصا؛
- يقوم الزبون استخدام النقود الالكترونية وفق الحاجة بالتعامل مع البرنامج الذي يتيحه له ***Digi cash*** وإرسالها مخفية للبنك لاعتمادها؛
- يوقع البنك على وحدة النقود بعد خصم قيمتها من حساب الزبون ثم إرسالها عبر الانترنت؛
- يقوم الزبون بنقل قيمة النقود إلى حساب التاجر المستفيد عبر الشبكة حسب الطلبات؛
- المستفيد يراجع البنك المصدر للتأكد من صلاحية النقود المستخدمة وبعدها يودع قيمتها في بنكه؛
- يقوم البنك المستفيد من بإجراء مقاصة مع البنك المصدر لقيمة النقود الالكترونية المتعامل بها؛
- يخزن البنك المصدر الرقم التسلسلي للنقود في قاعدة معلومات للتأكد من عدم صرفها مرة أخرى بطرقة احتيالية.

3.1. نظام الـ *Mondex*: ولد نظام ***Mondex*** خارج الشبكة ***off – Line*** وبدأ يهاجر نحوها، وهو نظام أساسه البطاقات ذات الشريحة الالكترونية التي يمكن أن تجري تحويلا ت فيما بينها دون استلزام وجود مراجعة أو تسوية بواسطة احد البنوك، كما يمكن إعادة تحميل بطاقة ***Mondex*** الذكية بقيم نقدية جديدة، ولهذا تعتبر هذه النقود الأقرب للنقود الالكترونية[17].

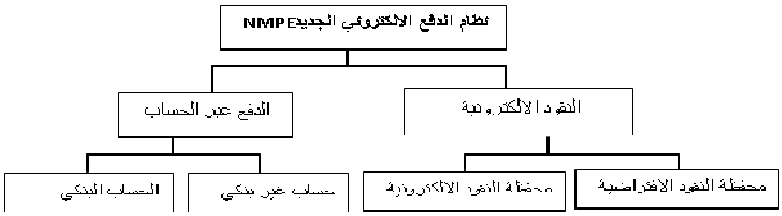
وبهذا فإنه يجري وضع كل الوسائل الممكنة من بطاقات ونقود الكترونية واستخدام شبكات الانترنت لإتاحة الدفع والتداول، حيث يمكن التمييز في وسائل الدفع المصرفية التالية كنظم دفع جديدة[18]:

- **الدفع خارج الشبكة *Les Paiement Hors Ligne*:** بإجراء عملية شراء عبر الانترنت وإرسال النقود عن طريق البنك أو شيك لتسوية المعاملة.
- **الدفع عبر الانترنت بواسطة بطاقة بنكية *Le Paiement en Ligne par Carte Bancaire*:** وهو أكثر النظم استعمالا حيث يتم تسوية المعاملة بواسطة أحد البنوك بين البائع والمشتري.
- **نظام القرض الاستهلاكي عبر الانترنت *Les System de Crédit à la Consommation en Ligne*:** وهي تقنية حديثة نسبيا عن طريق فتح خط دفع بالأجل (منح قرض) لشراء المبيعات عبر الانترنت بعد إعطاء بيانات المتعامل وبريده الالكتروني وكلمة المرور التي تتضمن العملية وتمنح الائتمان، ومثال على هذه التقنية شركة ***euro.com***.
- **نظام الدفع الجزئي عبر الانترنت *Le Système de Micro-paiement en Ligne*:** يسهل عمليات الدفع من خلال دفعات المبالغ الصغيرة، وهو جد مهم للذين لا يرغبون في تقديم بيانات وتفاصيل عن حساباتهم المصرفية، ويشمل هذا النظام جانبين الدفع عن طريق ***SMS*** بإرسال بيانات الدفع إلى البنك، ويتم التأكد من الصفقة من البائع الذي يرسل رمز الوصول وترخيص المعاملة وبالتالي يتم الاقتطاع والتسوية، أو عن طريق المحفظة الالكترونية ***Le porte-monnaie électronique*** حيث يتم الخصم من حساب الدفع مباشرة من البطاقة أو عن بواسطة الآلية السابقة أو عن طريق تقنية ***SMS*** السابقة.
- **الحسابات الافتراضية على الانترنت *Le Compte Virtuel en Ligne*:** ويمكن أن تعمل البطاقة باستعمال أية وسيلة من وسائل الدفع السابقة، أو يتم تنفيذ الصفقة من خلال الخصم المباشر من الحساب الافتراضي بعد تقديم البيانات وتفصيل الحساب وتأكيدها.

هذا ومن المتوقع أن تحل النقود الافتراضية تدريجيا محل النقود الورقية عن طريق الخصم والتسوية بواسطة البطاقة أو الحساب المصرفي وتبادل البيانات والمعلومات الكترونيا، لا سيما عند

المعاملات بكميات صغيرة على الخط[19]؛ وبهذا يمكن فصل جميع وسائل الدفع الالكترونية إلى مجموعتين رئيسين والموضحة في الشكل التالي[20]:

الشكل رقم (01): وسائل الدفع الالكترونية الجديدة.



La source: *David Bounie, op cit, P 80.*

2. **أنظمة التحويل الالكترونية:** يتم تحويل الأموال والبيانات من خلال أنظمة الكترونية متطورة نفصلها في النقاط التالية[21]:

1.2. **نظام جمعية الاتصالات المالية العالمية بين البنوك *e-swiftsh*:** يقوم هذا النظام على شبكة ربط الكترونية بين فروع البنوك الواحدة بحيث يمكن للزبون من السحب أو الإيداع في حسابه لدى أي فرع دون الحاجة إلى الحضور للفرع الذي فتح فيه حسابه، ومن خلال هذا النظام يتم التحويل المالي بين الفروع وتبادل الرسائل الكترونيا عبر نظام مشفر وعلى درجة عالية من الإتقان والحماية والأمان.

2.2. **نظام مقاصة المدفوعات بين البنوك الـ *swift*** [22]: عبارة عن شبكة عالمية تربط البنوك العالمية ببعضها البعض لإرسال واستقبال الرسائل المالية وغير المالية تسهيلا لإجراء العمليات البنكية في إطار نظام الكتروني متطور، ويتم ذلك بشكل آمن في زمن لا يتعدى 10 ثوان حول العالم.

3.2. **نظام بيت المقاصة المؤقتة الـ*ACH*** [23]: هو نظام يستخدم لدفع الحوالات خلال يوم أو يومين، وتم تصميمه أصلا للحوالات الصغيرة والمدفوعات المتكررة، ويربط حوالي 12000 مؤسسة مالية ببعضها البعض وحوالي 40000 شركة وحوالي مليون مستخدم لهذا النظام. وعادة ما يستخدم النظام لدفع الرواتب واستحقاقات التقاعد وتحصيل أقساط التامين والدفعات العادية، وما يميز نظام ***ACH*** انه يحول الأموال مرفقة بعدد قليل من الشروحات التابعة للتحويل من جهة ومرونة النظام في تسوية الصفقات خاصة التي تتعامل مع قياس الاكس.

4.2. **نظام الحوالات التلغرافية *Wire Transfer*:** يتيح هذا النظام تسوية المدفوعات ودفع الحوالات المالية من خلال اليوم عينه وبطريقة فورية بين الشركات والمستهلكين، بإعتباره نظاما مصمما

لاستيعاب تحريك الأموال بصورة سريعة ومؤكدة، لكنه لا يحتوي على أي معلومات أو شروحات، إذ يحتوي فقط على وجهة الدفعة ويستخدم فقط في الحوالات ذات المبالغ العالية.

5.2. **أنظمة تحويل أخرى:**

أ. **نظام العقود الالكترونية الآمنة *SET***[24]: هو نظام يضمن أمن العقود الالكترونية والصفقات التجارية على الانترنت، تم تطوير هذا النظام بدعم من شركات ***MasterCard*** و ***Netscape*** و ***Visa*** و ***IBM*** وغيرها، يستخدم نظام ***SET*** نظام الأقفال والمفاتيح، بالإضافة إلى رقم حساب معتمد لكل من الزبون والشركة التي تزاول أعمال التجارة الالكترونية على الانترنت، وتكون هذه الإجراءات بمثابة ضمان للزبون حول حقيقة الموقع الذي سيقوم بالتعامل معه[25].

ب. **نظام التحويل المالي الالكتروني *EFT***[26]: هو نظام التحويل بين الشركات نفسها أو بين الشركات والأفراد، ويتيح هذا النظام تحويل وتحريك الأموال وجميع أنواع المدفوعات إما بالشيكات أو بالطرق الالكترونية[27]، وعلى الرغم من شيوع هذا النظام إلا أنه صمم لتحويل قيم من الأموال من حساب إلى آخر ويمكن أن يتم ذلك بواسطة جهاز الصراف الآلي أو الحاسوب الشخصي أو طرف الهاتف، ويؤيد العديد من البنوك الالكترونية التحويلات التي تعتمد على الانترنيت بواسطة هذا النظام إلا أنه يحتاج للنظام السابق ***SET*** لإتمام العمليات البنكية بطريقة آمنة[28].

III. **الحاجة لحماية أنظمة الدفع:** أكثر ما يقلق القطاعات المصرفية بشأن استعمال للتقنيات المستجدة هو خطر الجرائم الالكترونية والجماعات الإجرامية المتخصصة بتزوير البيانات وسرقة المعلومات الشخصية. وسنقف هنا على جملة التهديدات والمشاكل والتحديات الفنية والتقنية التي تستدعي حماية أنظمة الدفع الالكترونية بالبنوك وتبرز الحاجة إلى الحماية والأمن لسلامة هذه التعاملات في النقاط التالية:

1. **الحوادث والأعطال:** إن احتمال إخفاق أنظمة المعلوماتية وتعطلها أصبح واقعا أكيدا بالرغم من عدم البوح بذلك حفاظا على "**صورتها المميزة**"، وتتنوع أسباب هذه الحوادث فمنها المادية (الحريق، التسرب المياه...إلخ) ومنها التقنية (أعطال، انقطاع التيار الكهربائي...إلخ) أو ذات الطابع الإجرامي (كالتخريب والقرصنة...إلخ)؛ في كل الأحوال هذه الحوادث قد تعطل العمل في جهاز المعلوماتية المصرفية كليا أو جزئيا ولفترة يمكن أن تقصر أو تطول[29]، ويمكن تقسيمها إلى الأنواع التالية[30]:

1.1. **الأخطاء في التنفيذ وسير الخطوات:** وسبب ذلك هو أن مشغلي البرامج لم يسيروا على المسار الصحيح لهذا البرنامج. وبالتالي تظهر نتائج غير صحيحة، ويعتقد مستخدمي البرامج فيما أن هناك عطلا ما في البرنامج خاصة في بدايات التشغيل حيث يكون خطا في البرنامج نفسه.

2.1. **أعطال الأجهزة:** تتفاقم الأعطال دون أن يصدق هذا المستخدم أن العطل الصغير قد يتسبب في مشاكل خطيرة وتصيب هذه الأعطال أجهزة الـ ***harware*** ما يحدث مشاكل كبيرة في النظام.

3.1. **الخطأ في البرمجة:** ويمس برامج الـ ***software*** ويتسبب في إظهار نتائج غير صحيحة ولا تتماشى مع الواقع، وعلى الرغم من مراجعة المشغلين لكافة البرامج والتأكد من جميع الخطوات المحددة سليمة إلا أنهم يجدوا في بعض الحالات نتائج لا تتوافق وسير النظام سببه الخطأ في البرمجة.

4.1 **إدخال بيانات بصورة خاطئة:** ويتم ذلك من قبل مستخدمي النظام وينتج عند إدخال بيانات غير صحيحة أو بصورة خاطئة وقد يحدث ذلك بسبب وجود بيانات متكررة أو ناقصة أو أن يقوم بإدخالها لأكثر من مرة مما يؤدي إلى ازدواج البيانات وينتج الخطأ في النظام.

5.1.**الخسائر المادية في أجزاء الكمبيوتر**: قد يحدث بعض الأعطال أو الدمار في بعض أجزاء الكمبيوتر كالقرص الصلب أو الذاكرة أو المعالج ما يؤثر على البيانات وربما تلفها والقضاء عليها.

6.1. **أداء النظام غير ملائم**: عندما لا يعمل الحاسوب بالطريقة التي ينبغي أن يعمل بها، ويكون ذلك بسبب الضغط الكبير عليه وكمية الأوامر التي تصدر من أكثر من شخص في آن واحد، ما يتسب في بطئ العملية أو إلغاءها تماما.

2. **الفيروسات**: هي عبارة عن برامج لها أهداف تدميرية بإحداث أضرار جسيمة بنظام الحاسوب، سواء بالبرامج أو الأجهزة ويستطيع أن يعدل ويركب البرامج الأخرى حيث يرتبط بها ويعمل على تخريبها وهو قادر على التوالد والتناسخ وله أفضلية على نظم التشغيل والتمركز فيها[31]. ويفوق عددها الثلاث آلاف فيروس، وما ساعد في انتشارها عمليات القرصنة المعلوماتية، والانتشار الواسع لشبكة المعلومات[32]. وتنقسم الفيروسات لعد أقسام أهمها:

1.2. **حسب طريقة انتشارها:** تنقسم الفيروسات حسب طريقة انتشارها إلى نوعين رئيسيين وهما[33]:

أ. **<u>الفيروسات المنتشرة عن طريق نظام التشغيل</u>**: هي الأكثر انتشار لان نظم التشغيل تضمن لها حرية كاملة بالأجهزة العاملة في هذا النظام " التشغيل" وتعمل بصورة متوافقة فيما بينها، وتتفرع فيروسات هذه المجموعة إلى **الفيروسات المنتشرة عن طريق *DOS*** وهي قديمة وتتواجد في الذاكرة ***RAM*** وتقرأ الملفات من نوع ***Com* و*Exe*** ... وتقوم بتغييرها أو إضافة نفسه إليها، ومع قلة هذا النوع إلا

انه قد يسبب في أخطار كبيرة للنظام؛ و**فيروسات الشبكات التي تنتشر عبر خطوط الاتصالات** التي تنتشر عند وجود شبكات محلية **Local Net** وكبيرة ***Globale Net*** متطورة وكذا وجود أنظمة وبرامج متقدمة.

ب.الفيروسات المنتشر عن طريق أقسام الجهاز نفسه: تنتقل من البرامج والاسطوانات الحاملة لها عن طريق أبواب العمليات المركزية ***Processor Part*** إلى الاسطوانات الأخرى، وهي أكثر صعوبة في الإخفاء والمقاومة كما يرسل نسخ منه حاملة للعدوى إلى كل رسالة تصله كما قد يعمل على تحطيم جدول تجزئة القرص وبدأ التشغيل ويستطيع أن ينتشر عبر كافة أنحاء العالم عبر شبكة الانترنت.

2.2. من ناحية الضرر الذي تحدثه: وتنقسم بدورها إلى عدة أقسام أهمها[34]:

أ. الجرثومة المعلوماتية: وهي شبيهة بالفيروس البيولوجي من حيث عمله لناحية الانتشار السريع والتكاثر حيث ما يحل، يتضمن أهداف تدميرية، ويتميز بقدرته على نسخ نفسه في البرنامج الذي يصيبه والتحكم فيه وتعديله، ويرجع سبب انتشار هذا الفيروس للاستعمال المكثف للشبكات الخاصة بالبريد الالكتروني وعلى الصعيد التجاري عبر أنظمة الشركات والبنوك.

ب.القنبلة المعلوماتية: هو برنامج يعده مصمم النظام المعلوماتي ويثبته بداخله، وينطلق هذا البرنامج بعد انقضاء مدة محددة على استعمال النظام بهدف تعطيله أو تدميره أو محو البيانات التي يحتويها، ويكثر استعمالها في الشركات التجارية والبنوك ويقف خلفها في الغالب موظفون وتقنيون من الداخل.

ت.الدودة: وهي عبارة عن برنامج معلوماتي يمتاز بقدرته على التنقل عبر شبكات المعلومات بهدف إعاقة عملها والتشويش عليها من خلال شل قدرتها على التبادل، هذا النوع من الفيروسات يتطلب التدخل السريع وإلا سوف يحدث أضرار جسيمة.

3. الجرائم المعلوماتية: برز للوجود نوع من الجرائم وهو ما يصطلح عليه بالجرائم الالكترونية ومجالها جهاز الكمبيوتر لاختراق شبكة الانترنت، وتعرف الجريمة الالكترونية حسب ما أقره المؤتمر العاشر للأمم المتحدة بأنها جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام الحاسوب وتشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية[35].

1.3.أصناف مجرمي المعلوماتية إن هذه الجرائم الحديثة والمستحدثة تتنوع وتتضاعف يوما بعد يوم ويختلف مرتكبوها عادة عن المجرمين التقليديين لأنهم في الغالب أشخاص على مستوى عالي من العلم والمعرفة "بالمعلوماتية" وقد يكون بعضهم من صغار السن ولكنهم ذو دراية تامة بأسلوب هذه الجرائم. ويمكن تصنيف هؤلاء المجرمين إلى الفئات التالية[36]:

أ. القراصنة: وهم على صنفان **الهواة *Hackers*** الذين يسعون للتسلية بدافع الفضول ولا يشكلون خطر على الصناعات وأنظمة المعلومات؛ و**المحترفون *crackers*** وهم أكثر خطورة من الصنف الأول وقد يحدثون أضرارا كبيرة وقد يؤلفون أندية لتبادل المعلومات فيما بينهم.

ب. المخادعون: يتمتعون بقدرات فنية عالية باعتبارهم من الاختصاصيين في المعلوماتية ومن أصحاب الكفاءات وتنصب معظم جرائمهم حول شبكات تحويل الأموال، ويمكنهم التلاعب بحسابات البنوك أو فواتير الكهرباء والهواتف أو تزوير بطاقة الاعتماد أو ما شابهها.

ت. الجواسيس: يهدفون لجمع المعلومات لمصلحة دولهم أو مصلحة بعض الأشخاص أو الشركات التي تتنافس معهم.

2.3. أنواع وتقنيات الجرائم المعلوماتية: نظرا لاعتماد المصارف الكبير والمباشر على تقنيات المعلوماتية والاتصالات المتطورة في إدارة أعمالها وتسيير أمور زبائنها، كان طبيعيا أن تتعرض البنوك لاعتداءات وجرائم جديدة مصدرها التقنيات الحديثة المستعملة، ويمكن إجمالها في التالي:

أ. جرائم الاحتيال المعلوماتي: تعددت تعريفات جريمة الاحتيال المعلوماتي وتعددت تسمياتها فاستخدم بعض الفقهاء تسمية الغش المعلوماتي واستخدم البعض الآخر تسمية غش الحاسوب، ولكن التعريفات تلتقي جميعها حول وصف هذا الجرم بأنه سلوك احتيالي أو خداعي مرتبط باستخدام الكمبيوتر يهدف مرتكبه على تحقيق فائدة أو مصلحة مالية. وقد نشأت هذه الجرائم بشيوع أنظمة نقل وتحويل الأموال الكترونيا ***EFT*** حيث تزايدت بشكل ملحوظ قيمة الأموال المتداولة بهذا الأسلوب مما جعلها تصبح موضوعا لجرائم التحويل الالكتروني غير المشروع للأموال[37].

ب. جرائم التخريب: التخريب هو كل عمل من شأنه أن يلحق ضررا بشيء ما فيؤدي إلى إفساده وانعدام جدواه، وقد يقع على الأجهزة (***Hardware***) كالطابعة أو الماسحة الضوئية...؛ أو البرامج ***Software*** والمعلومات، وإن كان المقصود بتخريب البرنامج هو تخريب القرص الضوئي أو الأسطوانة التي استعملت لتخزين المعلومات، فإن المقصود بهاته الجرائم هو الاعتداء على البرنامج نفسه باعتباره مجموعة من المعطيات واللوغاريتمات أو إجراء بعض التعديلات ما يحدث ضررا بها.

ت. جريمة التزوير والتلاعب: ويقع التزوير على مستندات مخزنة في ذاكرة الكمبيوتر لاستعمالها أو التلاعب بمحتوياتها بشكل مباشر أو غير مباشر فيدخل المعلومات في النظام الآلي لمعالجة البيانات أو يمحو أو يعدل في طريقة معالجتها أو نقلها، ويلجأ إلى هذه العمليات بعض الموظفين العاملين في القطاع المصرفي بإدخال معطيات مصطنعة للاستيلاء على الأموال بكميات صغيرة أو من خلال اقتطاع قيمة

صغيرة من الإيداعات بشكل لا يلاحظ نقصانها[38]. وطبقا لتصنيف معهد العدالة القومي للولايات المتحدة الامريكية فقد صنف الجريمة المعلوماتية في الأصناف المعلوماتية التالية[39]:

- **جرائم الكمبيوتر الداخلية**: ويقصد بها تعديل برامج الكمبيوتر بصورة ينتج عنها أداء الكمبيوتر لوظائف غير المسموح بها وذلك من خلال ذات البرامج ومن أمثلتها (محو البيانات أو التلاعب بها).
- **جرائم الاتصال**: ويقصد بها الاستخدام غير المشروع لأنظمة الكمبيوتر بمحاولة إيجاد الشفرة الصالحة والمناسبة لاقتحام البرنامج وذلك من خلال الاتصال المستمر بهذا النظام مستخدما العديد من الشفرات العشوائية والبرامج الدخيلة بشكل غير مشروع، حيث أن استخدام الشفرات المولدة عشوائيا بواسطة تلك البرامج يعد من قبيل الملكية المسروقة ومن أمثلتها الاحتيال التلفوني، الاستخدام غير المشروع، نشرات البيانات غير المشروعة، إساءة استخدام أنظمة التلفونات.
- **جرائم التلاعب في الكمبيوتر**: ومن أمثلتها الاختلاس والاحتيال، وتتضمن هذه النوعية من الجرائم تغيير البيانات أو إنشاء ملفات في أحد الأنظمة من أجل الإعداد لجريمة أخرى وغالبا ما تكون هذه جريمة السرقة، فكافة عمليات الاختلاس في المؤسسات المالية تتطلب إنشاء ملفات أو حسابات زائفة أو تعديل بيانات الكمبيوتر من أجل إخفاء الجرم المرتكب.
- **دعم التعاملات الإجرامية**: وهنا تلعب الأنظمة دورا محوريا في دعم العديد من الأنشطة الإجرامية مثل شيكات غسيل الأموال وعمليات المخذرات وقواعد بيانات للاحتفاظ بسجلات لتعاملات الزبائن.
- **سرقة البرامج الجاهزة والمكونات المادية للكمبيوتر**: وتتضمن هذه الجريمة عمليات نسخ البرامج دون تفويض أو سداد القيمة المقابلة لها.

4. الخصوصية وأدلة الإثبات: يطرح موضوع الخصوصية أو الخرق غير المرخص للحرية الشخصية تحديا آخر يستدعي الحماية منه في المصارف، ويمكن تحديد مفهوم الخصوصية حسب القانون الأمريكي بالتعدي غير المبرر على حرمة شخص آخر أو الاستيلاء على اسم شخص آخر أو كنيته أو الإشهار غير المبرر للحياة الخاصة للشخص الآخر أو الدعاية غير المبررة فتظهر شخص آخر بصورة مغلوطة أمام الجمهور، فقد أصبح مشكل الخصوصية في البيئة المعلوماتية يرتدي أهمية كبرى لأن التقنية المعلوماتية جعلت جمع وتخزين ومعالجة واسترجاع ونشر المعلومات الشخصية أمرا سهلا ومتاحا للجميع أكثر من أي وقت مضى، وقد تكرس هذا المبدأ منذ أمد واعتمدته غالبية دول العالم، لكن واجب السرية ليس مطلقا إذ غالبا ما تنص القوانين الوضعية على حالات محددة يسمح بها للمؤسسات المالية بكشف بعض المعلومات المتعلقة بزبائنها[40].

هذا في حقل الخصوصية، أما في جانب الإثبات فتثار مسألة الحجية التي يجب أن تمنح للوثائق التي تخرج من الحاسب الآلي وكذا حجية الأوعية التي تحتوي بيانات ومعلومات نقل الأموال كالأشرطة والاسطوانات الممغنطة والمصغرات الفيلمية. وأخيرا قيمة المعلومات المختزنة في ذاكرة الحاسب الآلي. هل تصلح أيا من هذه العناصر كأداة للإثبات؟، لا شك أن المسألة محل نقاش.

وفي محاولة لإعطاء مثل هذه العناصر بعض الحجية أصبحت العقود المبرمة بين البنوك والزبائن تتضمن نصا يجعل من هذه العناصر أداة لإثبات العمليات التي تسجلها. ورغم شرعية مثل هذه الاتفاقيات إلا أنها ولا شك مجحفة بالنسبة للزبائن. والحقيقة أنه يصعب على الزبائن إثبات عكس ما تدعيه البنوك استنادا للبيانات المستخرجة من الحاسب الآلي. وإن كان من غير المقبول من ناحية أخرى أن يعتمد البنك على أدلة مستخرجة من أجهزة تعمل تحت إشرافه وإدارته وله كامل التحكم فيها دون أي تدخل أو رقابة من جانب الزبون. فهل يمكن أن يعتمد البنك ويستند فقط إلى كفاءة الآلة.

وتدخل في الصعوبات أيضا مسألة إثبات حقيقة المعاملة وقيمتها ووقت أداءها، وهذه المسألة تثور بالنسبة لبطاقة الدفع نظرا لعدم وجود توقيع عليها، كما تثور أيضا على المعاملات التي تتم عن بعد كالأوامر التي تمر عبر الهاتف أو الحاسب الآلي المنزلي المتصل بحسابات المحلات أو البنوك. كما تثار في هذا الصدد أيضا مشاكل في الإثبات نتيجة عدم التعامل بأدوات الدفع التقليدية في صورتها الورقية، بل وقد وصل الأمر بالنسبة للشيك مثلا إلى التخلص منه بعد فترة زمنية محددة بعد إتمام عملية الوفاء والاحتفاظ بصورة له في شكل إلكتروني الأمر الذي يثير مسألة حجيتها في الإثبات[41].

IV. **أنظمة الحماية والأمان:** نظرا للمشاكل والتحديات السابقة استدعى على البنوك تطوير أساليب للحماية والأمان ولم تقف عاجزة أمام هذا الوضع، وبالرغم من شيوع أدوات الحماية والأمان إلا أنها لا تزال تتطلب التطوير المستمر كون أن عمليات الهجوم والاختراق عملية مستمرة. وسنتطرق هنا لطرق الحماية والأمان في أنظمة الدفع الالكترونية على النحو التالي:

1. **مدخل لأنظمة الحماية والأمان:** سنعرج في هذا الجانب لمفهوم أنظمة الأمن ونبذة تاريخية عن تطور هذه الأنظمة، وسنفصل في أنواع نظم الحماية في النقاط الرئيسية التالية:

1.1. **نبذة تاريخية عن أنظمة الأمن**[42]: إن التطورات المتعاقبة والسريعة أدت إلى ظهور أمنية المعلومات منذ البداية ووصلت الآن إلى نقطة عالية من التعقيد والاهتمام. ومرت بالمراحل التالية:

أ. **أمن الحواسيب *computer Security* *(الخمسينات والستينات)***: كانت الحواسيب في البداية تشغل من قبل نفس الأفراد الذين أعدوا البرامج وصيانتها، وكانت أهم إنشغالاتهم كيفية تنفيذ

الأجهزة للإيعازات المطلوبة منها، ولم يكونوا مشغولين بأمن المعلومات بقدر انشغالهم بعمل الأجهزة، ولذلك كانت الأمنية تدور حول تحديد الوصول أو الاطلاع على البيانات من خلال منع الغرباء بالتلاعب في الأجهزة،

ب. أمن البيانات *Data Security : (السبعينات)* تغير التركيز في الأمنية ليمثل السيطرة على البيانات وحمايتها. وتم الانتقال إلى **أمن البيانات**، ورافق ذلك استخدام كلمات سر بسيطة للسيطرة على الوصول إلى البيانات بالإضافة إلى إجراءات إضافية لحماية مواقع الحواسيب من الكوارث واعتماد خطط استرجاع سريعة للبيانات وخزن نسخ إضافية لهذه البرمجيات بعيدا عن موقع الحاسوب.

ت. أمن المعلومات *Information Security* في مرحلة ***(الثمانينات والتسعينات)*** أدى التركيز على المعالجات الدقيقة إلى انتقال الأمنية من البيانات إلى المعلومات، والمحافظة على المعلومات وتكاملها وتوفرها ودرجة توفيقها وتقليص اختراق المعلومات أو التلاعب بها. وكانت شركة (***IBM***) الأمريكية أول من وضع تعريف لأمن المعلومات وقد تضمنت إحدى سياسات الشركة رقم 130 بأن أمن البيانات هو حماية البيانات من حوادث التحوير أو التدمير أو كشف المعلومات بدون تخويل، كما أشارت بأن أمنا تاما للبيانات لا يمكن تحقيقه، ولكن مستوى مناسب من الأمنية يمكن تحقيقه بإتباع أو التركيز على بعض العناصر والجوانب المهمة للأمنية. وقد اقترح مؤخرا ***Donn Parker*** من ***SRI International*** تعريفا جديدا لأمن المعلومات هو "حماية تكامل وإتاحة وموثوقية المعلومات" والسؤال الذي يطرح نفسه ماذا سيكون بعد أمن المعلومات؟ البعض يقول أمن المعارف ***Security Knowlodg*** سيكون موضوع أمن الحاسبات وذلك لانتشار الذكاء الصناعي وازدياد معدلات تناقل البيانات بسرعة الضوء والتفاعل بين المنظومات والشبكات وصغر حجم الأجهزة.

2.1. تعريف الأمنية *Security*: هي كافة الإجراءات المتخذة لمنع الفقدان بأي شكل من الأشكال مثل فقدان الخدمة أو فقدان البيانات[43]، وتتمثل في حماية المصادر من خلال تأمين الخدمات والمواقع الشبكية الشخصية من جهة وحماية نقل البيانات حيث لا يتم الاطلاع على محتويات الرسالة أو نسخها، بتأمين القناة أو الأدوات وتأمين الوثائق[44]، وعليه تتحدد الأمنية والحماية في ثلاث نقاط نسبية:

أ. الهجوم الأمني *Security Attack*: غايته كيفية منع الغش أو الفشل وكشف الخداع في أنظمة المعلومات، ويتطلب هنا احتواء الهجوم ومعالجته ورصد عمليات انتهاك السرية أو الخصوصية.

ب. آليات الأمنية *Security Mechanisms*: لا توجد آلية مفردة تؤمن جميع الخدمات المقاومة، على كل حال هناك عنصر محدد يساهم في جميع آليات الأمنية المستخدمة كتقنيات التشفير أو القياسات البيولوجية والجدران النارية... وسيتم شرح هذه التقنيات لاحقا.

ت. خدمات الأمنية *Security Services*: هي تكرار إلى أنواع الفعاليات المرتبطة بالمستندات المادية، والتي تعتمد في معظمها على فعاليات البشر في مجال التجارة والصيرفة الالكترونية والزبائن والبنوك...إلخ والتفاعل الشخصي لهؤلاء الفرقاء للمعاملات التي لها خصوصية في سلامة المستندات التي تحتوي بصمات وتواريخ وبيانات يجب حمايتها من التشويش أو السرقة أو التدمير.

إن بناء نظام يلبي متطلبات الأمنية يكون صعبا جدا بسبب أن المشكلة المطلوب معالجتها ليست ساكنة ***Static*** لكنها متحركة ***Dynamic***، فتأمين سهولة استخدام وسائل الاتصال ***Interface*** أو الاتصال المباشر ***Online*** أو التسهيلات المساعدة أو جدولة الزمن الحقيقي هي كلها متطلبات ساكنة. ويمكن تحديد الحل التقني لتلك المتطلبات عندما يتم بناء النظام وتسليمه إلى المستخدم، والمهم أن يكون صالح خلال فترة حياة النظام، ويعتمد الحل الأمني على العوامل التالية:

- **تهديدات النظام - تشابه التهديد المطبق في النظام.**
- **الحالة التقنية المتوفرة لحماية النظام. - قيمة موارد معلومات المؤسسة.**

فالحل الأمني هو جانب حركي حيث يمكن لتهديد البنك أن يتغير اعتمادا على أحداث محددة، ومن جهة أخرى لا تزال معظم الأنظمة الأمنية واهنة جدا أمام الهجومات والسبب الرئيسي في ذلك أن النظام الأمني مكلف عند إنشاءه ومزعج في تنفيذه. وتبقى نظم الأمنية مسؤولة عن تطوير وتنفيذ وصيانة برامج الأمن المعدة لحماية تكامل وإتاحة وسرية وتوفيرية المعلومات.

3.1. **مستويات الحماية والأمان:** تشمل أنظمة الأمان والحماية عناصر عديدة تتمثل في الآتي[45]:

أ. الحماية المصرفية التقليدية: ويقصد بها أنظمة الحماية التي يلجأ إليها المصرف لصون مراكزه من أية اعتداءات، فيصمم مبانيه بشكل ملائم ويضع الكاميرات في كل منطقة حساسة، هذا المستوى الأول من الحماية لجعل المعلومات الخاصة لمستعمل المصرف عبر الانترنيت من قبيل الاسم وكلمة المرور بمأمن من وقوعها بأيدي أشخاص ينوون استعمالها بطريقة غير مشروعة.

ب. حماية الأجهزة الالكترونية للبنك وملحقاتها: يتطلب حماية الحاسوب المركزي للبنك الموصول بشبكة الانترنيت، وإبقائها سرية، ويستعين البنك غالبا بتقنية تعرف بأسوار الحريق ***Firewalls***. وهو نظام مخصص لحماية المعلومات التي يختزنها الكمبيوتر. فيوجه رزم المعلومات إلى سور الحريق مباشر ويتحقق من مصدرها ويحدد وجهتها ثم يعطيها العنوان المناسب داخل الشبكة الداخلية للبنك مما يجنبها من أي احتكاك خارجي للتلاعب أو الاختراق.

ت. حماية أنظمة البنك أو البرامج: ويعني حماية أنظمة التشغيل وبقية الأنظمة والبرامج المنفذة وضمان الرقابة عليها وكشف أي تلاعب في وقت مبكر، بوضع تعليمات خاصة في تصميم النظم وكتابة البرامج ووضع عدد من الإجراءات كالمفاتيح الأمنية والعوائق، وتحديد صلاحيات الدخول وقراءة الملفات أو الكتابة عليها، وتحديد من لهم الحق في الاطلاع وبمستويات مختلفة، والنسخ الإضافي اليومي أو الأسبوعي أو الشهري لهذه البرامج والأنظمة وتحديثها.

ث. حماية المعلومات بين المستعمل والبنك: فضلا عن حماية الأجهزة والبرامج يجب اعتماد أسلوب لتشفير المعلومات التي تكون مفتوحة للجمهور عبر الانترنت، وتقنين البنوك بتقنية ***SSL Secure Socket Layer*** لحماية أنظمة التصفح عبر الانترنت حيث يتم التعرف على كل عملية اتصال يقوم بها المستعمل ويعطيها رمزا يضيفها لنظام التصفح للمحافظة على استمرارية التعاطي مع طالب واحد خلال عملية اتصال واحدة ما يمنع تحويل هذه العملية لطرف ثالث فيما لو تمكن كشف مفتاح التشفير.

ج. حماية الاتصالات والمواقع: تشمل منظومة الاتصالات وأجهزة التراسل بين الحواسيب وملفاتها وخطوط الهاتف... وذلك بإحدى الفحوصات الدورية وكشف التسلل والاعتداء باعتماد نظم الأقفال. ولضرورة اكتمال الإجراءات الأمنية لا بد من إعطاء أهمية للمواقع الالكترونية وتطبيقات نظم حمايتها وتحصينها من التخريب والسطو والتحقق من هوية الأفراد المتصلين.

ح. الحماية المتعلقة بالمستفيد من الخدمة: يمثل آخر حلقة في عملية الحماية لتكتمل منظومة الحماية بشكل نهائي، فالبنك مطالب بحماية المعلومات التعريفية المتعلقة بالزبون كالاسم والرقم السري وذلك كي لا يسقط في شخص آخر، كما يتوجب على المستعمل أن يكون على دراية تامة باستعمال الحاسوب الخاص به فيتعين عليه غلق الحاسوب بعد استعماله وتغيير كلمة المرور إذا كانت متاحة...إلخ.

2. التشفير *Cryptography*: يعود تاريخ التشفير إلى **4000** سنة حيث كان الإنسان يفضل أن يحمي كتاباته، ويمثل التشفير أهم وسائل وأنظمة الحماية التي تستعين بها البنوك وفيما يلي توضيح لآلية التشفير وطريقة عملها:

1.2. مفهومه: هو عبارة عن خوارزمية أو دالة رياضية لإخفاء المعلومات داخل أشياء أخرى أو ترميز الرسالة حتى يكون معناها غير مفهوم، أما فتح الشفرة فهو العملية المعاكسة للتشفير وتحويل الرسالة إلى شكلها الطبيعي[46]. كما تعرف بأنها الآلية التي يتم بمقتضاها ترجمة معلومة مفهومة إلى معلومة غير

مفهومة يمكن إرجاعها إلى حالتها الأصلية، ولا يقف دور هذه التقنية في سلامة وسرية المعلومات والمعاملات بل تلعب دورا أساسيا في تدعيم أدلة الإثبات المعلوماتي[47].

2.2. **تقنيات التشفير:** يمكن تقسيم تقنيات التشفير إلى نوعين أساسيين هما[48]:

أ. **تقنية التشفير المتماثل:** يسمى بتقنية المفاتيح الخصوصية التي تقوم على استخدام ذات المفتاح الخصوصي أو الرمز في تشفير وفك الشفرة. ما يعني وجود مفتاح واحد يمتلكه المرسل والمرسل إليه، وتصلح هذه التقنية في الأنظمة المغلقة حيث تقوم علاقة بين الأطراف تسهل معرفة هوية المصدر وعملية التأكد من المصدر. ويقل اعتماد البنوك عبر الانترنت على هذه التقنية.

ب. **تقنية التشفير غير المتماثل:** هي التقنية الأكثر استعمالا في المصارف لأنها تؤمن قدرا عاليا من الموثوقية، وتسمى بتقنية المفاتيح العمومية التي ترتكز على استعمال مفتاحين. أو رمزين مختلفين الأول خصوصي يعرفه مستخدم معين لشبكة الانترنيت ويبقى سريا وخاص، والثاني عمومي يجري توزيعه وإبلاغه للجميع الذين يرغبون في تلقي الرسائل من البنك. وتتمثل أقسام استخدامات التشفير في ثلاث عناصر أساسية وهي: *- تشفير/فتح التشفير ، - التوقيع الرقمي ، - تبادل المفتاح .*

وتصنف أنظمة التشفير بصورة عامة إلى الأصناف الرئيسية التالية:

- **نوع العملية المستخدمة لتحويل النص الواضح إلى نص مشفر:** تعتمد جميع خوارزميات التشفير على مبدأين عاميين هما: **التبديل *Substitution*** حيث يحول كل عنصر في النص الواضح إلى عنصر آخر، ***والتعويض Transposition*** بإعادة ترتيب عناصر النص الواضح للحصول على النص المشفر.
- **عدد المفاتيح المستخدمة:** إذا استخدم المرسل والمستقبل نفس المفتاح فإن المنظومة تعرف بالشفرة **المتناظرة *Symmetric*** أو المفتاح الواحد أو المفتاح السري وتسمى التشفير التقليدي، وإذا استخدم المرسل مفتاح يختلف عن ما يستخدمه المستلم فإن المنظومة تسمى **غير المتناظرة *Asgmmetric*** أو ذات المفتاحين أو تشفيرة المفتاح العام.

3.2. **متطلبات التشفير الآمن**[49]: يجب أن يتمتع التشفير ببعض المواصفات والخصائص حتى يكون نظام التشفير ناجحا ومن هذه المواصفات ما يلي:

- يجب أن يتحدد حجم السرية المطلوبة وحجم العمل المناسب للتشفير وفتحه.
- يجب أن تكون مجموعة المفاتيح وخوارزمية التشفير خالية من التعقيد (شفرة قصيرة).
- يجب أن يكون تنفيذه بسيط قدر الإمكان.
- يجب أن لا ينتشر الخطأ في التشفير ليسبب تدمير أكثر للمعلومات والرسائل.

- يجب أن يكون حجم النص المشفر ليس أطول من النص الأصلي للرسالة.

بالإضافة إلى المواصفات السابقة يوجد مبدأين إضافيين لهما علاقة بحجم العمل لانجاز التشفير، **الأولى متعلقة بخوارزمية التشفير** التي يجب أن تأخذ المعلومات من النص الواضح وتحولها حيث لا يستطيع المتطفل أن يميز الرسالة بسهولة. **والثاني التشويش *Confusion*** حيث لا يكون هناك القدرة للمتطفل لتوقع ماذا يعنى تغيير رمز واحد في النص الواضح وتأثيره على النص المشفر.

3. **القياسات البيولوجية:** تطور حقل القياسات البيولوجية ***Biomitrics*** بصورة مستمرة مما جعل البنوك تعتمد على تقنيات القياسات البيولوجية للحصول على الأنظمة الأمنية.

1.3. تعريفها: يعتمد تعريف القياسات البيولوجية على خصائصها وعلى مؤهلات القياسات الحسابية، وهي تستند إلى طرق التحقق البيولوجي كهندسة اليد ورسم الشبكية وبصمة الأصابع والإثبات الصوتي وتمييز الوجه وهندسة الإصبع، والجدول التالي يوضح القياسات المستخدمة:

جدول رقم (01): القياسات البيولوجية المستخدمة

السلوكية			الفسيولوجية		
التوقيع	حركة شفة الفم	انعكاس الجلد	الوجه	DNA	شبكة العين
الصوت	حرارة الجسم	قرنية العين	بصمة الأصابع	شكل الأذن	رائحة الجسم
المسير	ضربة مفاتيح الإدخال		هندسة اليد		

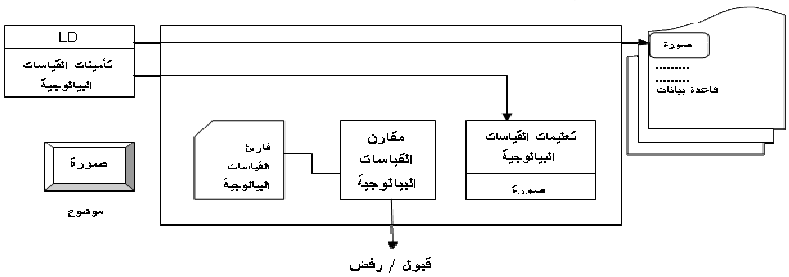
المصدر: علاء حسين الحمامي وسعد عبد العزيز العاني، مرجع سبق ذكره، ص 268.

من خلال الجدول نجد أن هناك ثلاث طرق رئيسية للتحقق من التعريف: **شيء تعرفه** مثل كلمة المرور أو جملة المرور، **شيء تملكه** مثل البطاقة الذكية، وأخيرا **شيء خاص بك** مثل ميزة قياسية كطبعة الأصبع.

2.3. تقنياته: ينتج عن نظام تعريف القياسات البيولوجية مطابقات عديدة للموضوع المطلوب، وتختلف عملية التعريف عن الإثبات في أن القياسات البيولوجية تقارن فقط مع مدخلة واحدة مسجلة من القياس، فقد يكون هناك عدد كبير من المجتمع المسجل لكن المستفيد يقدم رمزا يشير إلى طبعة واحدة من القياس البيولوجي مرتبطة مع هوية الموضوع، وناتج هذا القرار هو الرفض أو القبول. وتتم هذه العملية أولا بتسجيل القياسات البيولوجية، وهي عبارة عن عملية تسجيل المواضيع في

قاعدة بيانات القياسات البيولوجية، وتشمل عملية تسجيل المعلومات المتعلقة بالمستفيد كشهادة الميلاد وجواز السفر والبيانات الأخرى للمستفيد لتطابق مع القياسات البيولوجية، كما يوضحه الشكل التالي:

الشكل رقم (02): تسجيل واثبات القياسات البيولوجية



المصدر: علاء حسين الحمامي وسعد عبد العزيز العاني، مرجع سبق ذكره الصفحة .280

3.3. أمنية نظام القياسات البيولوجية*Biometric System Security*[50]: يكمن أمان التطبيق الذي يتحقق من خلال القضاء على الوهن في نقاط الهجوم من خلال الحماية ضد التقاطع ***Interception*** ؛ فبالنسبة إلى تطبيق مالي أو نقدي فإن المهم هو المال. وبالنسبة إلى تطبيق نقل المسافرين فإن المهم هو نظام النقل والمسافرين، فيكون الشيء الواجب حمايته هو البشر والتهديد هم البشر أيضا. وتتميز القياسات البيولوجية عن سياقات التحقق التقليدية بطرق عديدة. حيث تقدم معلومات القياسات البيولوجية عندما يكون " المالك " غير حاضر. فيتم تحقيق ذلك من خلال رفع طبعات الأصابع من المواضيع الأصلية إلى استخدامها في أعمال عدوانية مثل قطع الأصابع.

هناك فرق كبير في صعوبة استخدام المعرفة حول القياسات البيولوجية مقابل استخدام المعرفة حول كلمة السر للوصول غير المخول. فحتى إذا تم خداع الماسح **Scanner** لطبعة الإبهام بكل سهولة باستخدام قياسات بيولوجية خادعة. إلا أن انتحال قياس بيولوجي هو أبدا ليس بسهولة انتحال شخصية من خلال استخدام كلمة المرور المسروقة. غير أن التحقق هو أضعف نقطة لأنها الأكثر والأسهل في الهجوم. ويتوقع أن يهاجم المتطفل نقاط الوصول الأقل حماية. وعليه فالتحقق للقياسات البيولوجية يجب أن يكون موضوع متكامل مع الأمنية بأجمعها في التطبيق، والتي تتضمن منع اختراق الأمنية لنظام القياسات البيولوجية نفسه؛ وتتلخص أبرز **مشاكل القياس البيولوجي** في الآتي[51]:

- صور البيومتري توضع على القرص الصلب للحاسوب ***Disk Hard*** وبالتالي يمكن مهاجمتها أو نسخها بواسطة الطرق المختلفة المستخدمة في القرصنة الالكترونية أو نظم فك التشفير والترميز.

- عدم تمكن استخدام هذه التقنية الحديثة في كل الحواسيب نظرا لاختلاف نظم التشغيل وأساليب التخزين وخصوصيات حزم البرامج المتنوعة (***Lack Of Interoperability***).
- فقدان السرية والكفاءة الضمانية لهذه التقنية نظرا لمحاولة الشركات المصنعة لنظم البيومتري الاتفاق على طريقة موحدة (***Standard***) لهذه التقنية.

وعلى الرغم من أن معظم الشركات المصنعة لنظم البيومتري تعلن أن نسبة دقة عمل منتجاتها، أي التحقق من الشخصية (***Accuracy***)، تتراوح من 99 % -99.9% إلا أنه من غير الممكن التأكد من هذه النسب المرتفعة نوعا ما، حيث يوجد حاليا حالات احتيال باستخدام البصمة الشخصية المقلدة البصمة البلاستيكية والمطاطية (***Latex Rubber Fingers***) وعدم استطاعة أجهزة التحقق البصرية المصنوعة من رقائق السيليكون (***Silicon Sensor***) من كشفها أو تمييزها.

4. **التوقيع الالكتروني:** لعب التوقيع الالكتروني دورا رئيسيا في نمو عدد كبير من النشاطات عبر الانترنيت لما يوفره من أمان وحجية إثبات في المحررات الالكترونية، وتعتمد هذه التقنية على آلية التشفير والقياسات البيولوجية أو الاستعانة بالرقم السري...إلخ وسنوضح آلية التوقيع الالكتروني في التعامل المصرفي كأداة أمان في نظم الدفع على النحو التالي:

1.4. مفهومه: يشكل التوقيع الالكتروني محط اهتمام المصارف عبر الانترنيت لأنه يساعدها على التأكد من أن الشخص الذي يتعامل معها هو أحد زبائنها فعلا وليس أحد المتطفلين، ويعرف التوقيع الالكتروني بأنه رقم أو رمز سري أو شفرة خاصة لا يفهم معناها إلا صاحبه أو من يكشف له هذا الأخير عن مفتاح ذلك الترقيم أو الترميز أو التشفير[52]. أو هو إجراء معين يقوم به الشخص بتوقيعه على المحرر سواء احتفظ بالرقم السري أو الشفرة بشكل آمن وسري بمنع استعماله من قبل الغير، ويعطي الثقة بأن صدوره من صاحبه فعلا[53]. وأخيرا هو مجموعة الإجراءات أو الوسائل التقنية التي يتيح استخدامها عن طريق الرموز أو الأرقام بإخراج رسالة الكترونية يجري تشفيرها باستخدام خوارزم المفاتيح احدهما مشاع أو معلن والآخر خاص بصاحب الرسالة يحتفظ بسريته[54]. وهكذا فالتوقيع الالكتروني عبارة عن علامة مميزة لصاحب الرسالة المنقولة الكترونيا، له طابع متفرد يسمح بتحديد شخص الموقع ويميزه عن غيره.

2.4 . صور وأشكال التوقيع الالكتروني: يسود الاعتقاد بين العوام بوجود شكل واحد للتوقيع الالكتروني، لكن في حقيقة الأمر يأخذ صور وأشكال متعددة وذلك يعود من جهة إلى تقدم الوسائل التقنية التي أوجدها التطور التكنولوجي، ومن جهة أخرى إلى هاجس المحافظة على مستوى عالي من الأمان في طرق الدفع الالكترونية عبر الشبكات، وفيما يلي صور وأشكال التوقيع الالكتروني[55]:

أ. النسخ الالكتروني للتوقيع اليدوي: تتم هاته العملية بواسطة الموقع نفسه الذي ينقل توقيعه اليدوي جهاز الماسح الضوئي ***Scanner*** حيث يقوم بتصوير ونقل التوقيع العادي إلى جهاز الحاسوب ويحفظ التوقيع المنسوخ في ذاكرة الكمبيوتر ليتم نقله عند اللزوم إلى الوثيقة المراد توقيعها. وتظهر هذه الألية أنها سهلة إذ يكتفي الاحتفاظ بصورة عن التوقيع لإعادة نقلها إلى النص الالكتروني، إلا أنها غير آمنة على الإطلاق لأنها قد تكون في متناول كل من يستطيع استعمال الكمبيوتر، أو من يستولي عليه، لذلك فهذا التوقيع غير مستعمل على نطاق واسع وغير معترف به كتوقيع قانوني موثوق.

ب.التوقيع بالرمز السري أو بواسطة البطاقة البنكية: يتم هذا التوقيع بإدخال بطاقة ممغنطة أو ذكية في أجهزة الصراف الآلي أو نقاط البيع ثم إدخال الرقم السري، وبالرغم من أن البطاقة والرمز لا يمثلان توقيع بالمعنى التقليدي والرسمي للكلمة، كون أن التوقيع هو إجراء يعبر عن هوية صاحبه ويعكس إرادته بإحداث اثر قانوني معين. وهذا ما لا ينطبق مع البطاقة والرمز؛ ولتخطي إشكالية الثبوتية لهذه الوسيلة عمدت البنوك إلى إبرام اتفاق خاص مع الزبون للاعتراف بحجيتها التامة.

ت.التوقيع البيومتري: يرتكز هذا التوقيع على الدمج بين علم الأحياء القياسية وعلم المعلوماتية، ويعتمد على فكرة الاستخدام الالكترونية لعدد من المزايا العضوية التي تميز الأفراد بالإضافة إلى درجة وأماكن الضغط عند الكتابة أو التوقيع بواسطة الحبر، وهي جميعها أمور من شأنها إثبات الهوية في مجالات عدة، غير أن الكلفة المرتفعة لهذه الصورة من التوقيع إضافة إلى إمكانية تغيير بعض الخصائص العضوية لدى الإنسان مع تقدمه في السن، يجعلانها غير معتمدة على نطاق واسع.

ث.التوقيع الرقمي (التشفير): يرتكز هذا التوقيع على فكرة التشفير التي تتضمن سرية المعلومات والاتصالات وعدم إنكاره، ويعتمد على خوارزميات والمعادلات الحسابية الرياضية كمفاتيح خاصة أو عامة لأمان وموثوقية التعاملات لذلك يعتبر هذا النوع من التوثيق الأكثر انتشارا وشيوعا نظرا لسهولته وقلة كلفته بين سائر التواقيع السابقة.

خاتمة:

تبين من خلال هذه الورقة أن البنوك تسعى إلى تطوير نظم الدفع من خلال البطاقات البنكية المنتشرة والنظم النقدية الالكترونية المختلفة والموزعات الآلية المنتشرة عبر نقاط متعددة، وتطورت هذه الخدمات بصورة متزايدة ورهيبة وانفتحت على شبكات الانترنت وقنوات الاتصال الأخرى ما جعلها عرضة للتهديد والتطفل والاختراق، وفرض هذا الواقع على البنوك إيجاد أنظمة حماية وتطوير الدفاع ضد التهديدات المتكررة وكشف التطفل والهجوم والصيغ الأخرى في إساءة استخدام شبكة الاتصالات.

وعرضت هذه الورقة طرق حماية وأمان أنظمة الدفع الالكترونية وفهم عمل الأنظمة في مجال المعلوماتية والعمل المصرفي، وأوضحت آلية الأمنية وسلامة المعلومات والخصوصية... وعمليات الإجرام المعلوماتي. وبالرغم من التطور التكنولوجي في طرق الحماية والأمان إلا أنها لا تزال واهنة أمام التهديدات المحتملة كون أن هذه التطبيقات تمثل أهدفا جذابة للمجرمين والمخربين والمتطفلين، وما يتم اعتماده في الغالب إجراءات وقائية وليست حماية بالشكل المطلوب؛ وعلى العموم يمكن استخلاص أهم إجراءات الحماية والامان كمقترحات للدراسات في النقاط التالية:

- حفظ المستندات الالكترونية المحددة في شكلها النهائي طوال مدة صلاحياتها حيث يمكن الرجوع إليها دائما عند الحاجة.
- الصيانة الدورية لبرامج وأجهزة وعتاد البنك ومراقبة وسائل الاتصال بشكل مستمر. ونسخ وتخزين المعلومات في كمبيوتر خاص وتحديد الأشخاص الذين لهم صلاحية الدخول والتعامل به.
- اعتماد برامج مضادة للفيروسات أصلية غير مقلدة، ومتطورة، وتحديثها بشكل فوري.
- الدعم القانوني والتنظيمي لأدلة الإثبات وآليات التوقيع الرقمية من أجل إقرار وتنظيم أحكام الدفع الالكترونية ومتطلبات حمايتها.
- توفير الإمكانيات الفنية والتقنية على مستوى النظام المصرفي لتسهيل وإتمام عمليات الدفع الالكتروني ويتوقف ذلك على توافر الأجهزة المتطورة وإدارة المخاطر المرتبطة بها.
- نشر الوعي المعلوماتي ومحو الأمية في التعاملات الالكترونية، والتدريب المتواصل لموظفي المصارف كعملية مستمرة ضمن السياق المعلوماتي.
- تبادل الخبرات واستقطاب المؤهلات والكفاءات المختصة في مجال أنظمة الحاسوب، وتوسيع الجهود والتعاون والتنسيق مع الجهات العالمية التي تعتمد تلك الأنظمة.

وفي الختام ينبغي التأكيد على أهمية التقنية والمعلوماتية بالنظم المصرفية، إلا أنها تتطلب المزيد من الدراسات الاقتصادية والقانونية والتقنية لتطويع هذه التكنولوجيات بكل أمان واطمئنان لدى المتعاملين لا سيما عندما تقترن بالمال والأعمال، وهذا ما يزيد من مسؤولية ودور البنوك في حماية وأمن المعلوماتية.

هوامش البحث:

1 احمد سفر، **أنظمة الدفع الالكترونية**، منشورات الحلبي، بيروت، 2008، ص 20.

2 زهير بشنق، **العمليات المالية المصرفية الالكترونية**، اتحاد المصارف العربية، بيروت، 2006، ص240.

3نادر عبدالعزيز شافي، **المصارف والنقود الالكترونية**، المؤسسة الحديثة للكتاب، طرابلس، 2007، ص64.

4. زهير بشنق، مرجع سبق ذكره، ص 40.

5 . محمد رأفت عثمان، **ماهية بطاقة الائتمان وأنواعها وطبيعتها القانونية وتمييزها عن غيرها**، مؤتمر الأعمال المصرفية الالكترونية بين الشريعة والقانون، جامعة الإمارات العربية المتحدة، دبي، 10-12 ماي 2003، ص 616.

6 . موسى رزيق، **رضا حامل البطاقة الائتمانية بالعقد والحماية التي يقرها المشرع له**، مؤتمر الأعمال المصرفية الالكترونية بين الشريعة والقانون، جامعة الإمارات العربية المتحدة، دبي، 10-12 ماي 2003، ص 1038.

7 . ثناء أحمد محمد المغربي، **الوجهة القانونية لبطاقة الائتمان**، مؤتمر الأعمال المصرفية الالكترونية بين الشريعة والقانون، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، دبي، 10-12 ماي 2003 ، ص 946.

8. نزيه محمد الصادق المهدي، **نحو نظرية لبطاقة الائتمان من الوجهة القانونية**، مؤتمر الأعمال المصرفية الالكترونية بين الشريعة والقانون، جامعة الإمارات العربية المتحدة، دبي، 10-12 ماي 2003 ، ص 752.

9 **ATM** : Automatec Taller Machine.

10. وسيم حمد الحداد وآخرون، ص 64.

11. منظور أحمد حاجي الأزهري، **بطاقة السحب النقدي**، مؤتمر الأعمال المصرفية الالكترونية بين الشريعة والقانون، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، دبي، 10-12 ماي 2003 ، ص 357.

12 نبيل صلاح محمد العربي، **البنك الالكتروني والنقود الرقمية: دراسة مقارنة**، مؤتمر الأعمال المصرفية الالكترونية بين الشريعة والقانون، جامعة الإمارات العربية المتحدة، دبي، 10-12 ماي 2003 ، ص 70.

13محمد إبراهيم محمود الشافعي، **الآثار الاقتصادية والنقدية والمالية للنقود الالكترونية**، مؤتمر الأعمال المصرفية الالكترونية بين الشريعة والقانون، جامعة الإمارات العربية المتحدة، دبي، 10-12 ماي 2003 ، ص 134.

14محمود أحمد إبراهيم الشرقاوي، **مفهوم الأعمال المصرفية وأهم تطبيقاتها**، مؤتمر الأعمال المصرفية الالكترونية بين الشريعة والقانون، جامعة الإمارات العربية المتحدة، دبي، 10-12 ماي 2003 ، ص 29.

15. احمد جمال الدين موسى، **النقود الالكترونية وتأثيرها على دور المصارف المركزية في إدارة السياسة النقدية**، منشورات الحلبي، بيروت، ص 155.

16. محمد احمد إبراهيم الشرقاوي، مرجع سبق ذكره، ص 33.

17. احمد جمال الدين موسى، مرجع سبق ذكره، ص 156.

18Olivier de wasseige, **e- management ; e-commerce, e-marketing, e-Bay : 3 leviers de croissace pour les entreprise**, édition Pro, Belgique, 2007, P117.

19 Michel Badoc et autre, **e-marketing de la Banque et de l'Assurance**, 2eme edition, l'Organisation, Paris, 2000, P109.

20 David Bounie**, lorsque la sucurisation des payments par carte bancaire sur internet conduit à une concurrence entre les banques et les opérateurs de réseau**, annals des telecommunications : Commerce électronique le temps des evaluation; tome 58 n 1/2 , janvier – fevrier 2003; Paris, P 80.

[21] احمد سفر، **العمل المصرفي الالكتروني في البلدان العربية**، المؤسسة الحديثة للكتاب، لبنان، 2006، 157. احمد سفر، أنظمة الدفع الالكترونية، مرجع سابق، ص 20. وكذلك نادر عبدالعزيز شافي، مرجع سابق، ص 75.

22 **SWIFT**: Society for World Wide Interbank Financial Telecommunications.

23 **ACH**: Automated Clearing House.

24 . **SET**: Secure Electronic Transactions.

25. ناصر خليل، **التجارة والتسويق الالكتروني**، دار أسامة، عمان، ص 224.

26 .**EFT** : Electronic Funds Transfer.

27.عامر خطاب، **التجارة الالكترونية**، مكتبة المجتمع العربي، عمان، الطبعة الأولى 2006،ص 192.

28. عزة العطار، **التجارة الالكترونية بين البناء والتطبيق**، منشأة المعارف، الاسكندرية، 2003، ص 236.

29. شايب عينو الهادي، **الكمبيالة الالكترونية، القيد المضاد الالكتروني وخطأ المعلوماتية في إدارة الحسابات**، إتحاد المصارف العربية، بيروت 1991، ص 245.

30. نبيل محمد مرسي، **التقنيات الحديثة للمعلومة**، دار الجامعة الجديدة، الإسكندرية، 2005، ص342.

31. علاء عبد الرزاق السالمي ورياض حامد الدباغ، **تقنيات المعلومة الإدارية**، دار وائل، عمان، 2001.، ص 295.

32. القاضي وليد العاكوم، **مفهوم وظاهرة الإجرام المعلوماتي**، بحوث المؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، المجلد الاول، دبي، 1-3 ماي 2004، ص 20.

33. علاء عبد الرزاق السالمي ورياض حامد الدباغ، مرجع سبق ذكره، ص 300.

34. أمال عدنان يوسف، **إدارة المخاطر : التجسس التجاري- جواسيس المصارف والإجراءات الاحتياطية الواجب اتخاذها لحماية العملاء**- مجلة الدراسات المالية والمصرفية – الأكاديمية العربية للعلوم المالية والمصرفية، المجلد الثامن عشر، عمان، يونيو 2010، ص 38.

35. ربيحة زيدان، **الجريمة المعلوماتية في التشريع الجزائري والدولي**، دار الهدى، الجزائر،2011، ص 42.

36. القاضي وليد العاكوم، مرجع سبق ذكره، ص 12.

37. القاضي وليد العاكوم، مرجع سبق ذكره، ص 14.

38. أمال عدنان يوسف، مرجع سبق ذكره، ص37.

39. ممدوح عبد الحميد عبد المطلب، **جرائم استخدام شبكة المعومات العالمية " الجريمة عبر الانترنيت"**، بحوث المؤتمر القانون والكمبيوتر والانترنت، جامعة الامارات العربية المتحدة، دبي، 1-3 ماي 2004، ص 212.

40. أمال عدنان يوسف، مرجع سبق ذكره، ص35.

41.عصام إبراهيم القليوبي، **الجوانب القانونية الناجمة عن استخدام الحاسب الآلي في المصارف**، إتحاد المصارف العربية، بيروت 1991، ص117.

42. علاء عبد الرزاق السالمي ورياض حامد الدباغ، مرجع سبق ذكره، ص 249.

43.علاء حسين الحمامي وسعد عبد العزيز العاني، **تكنولوجيا أمنية المعلومات وأنظمة الحماية**، دار وائل، عمان، 2007، ص22.

44.علاء عبد الرزاق السالمي ورياض حامد الدباغ، مرجع سبق ذكره، ص 211.

45نهاد أبو جريش وغشان يوسف رشوان، **المدخل إلى مصارف الانترنيت**، اتحاد المصارف العربية، بيروت 2004، ص 98 - 106.

46. علاء حسين الحمامي وسعد عبد العزيز العاني، مرجع سبق ذكره، ص 91.

47. جورج نهاد أبو جريش وغشان يوسف رشوان، مرجع سبق ذكره، ص 103.

48. راجع كلا من: جورج نهاد أبو جريش وغشان يوسف رشوان، مرجع سبق ذكره، ص 106 وعلاء حسين الحمامي وسعد عبد العزيز العاني، مرجع سبق ذكره، ص 131.

49. جورج نهاد أبو جريش وغشان يوسف رشوان، مرجع سبق ذكره، ص 268.

50. المرجع السابق، ص 270.

51.عادل محمود شرف وعبدالله إسماعيل عبدالله، **ضمانات الأمن والتامين في شبكة الانترنت**، بحوث المؤتمر القانون والكمبيوتر والانترنت، جامعة الامارات العربية المتحدة، المجلد الأول، دبي، 1-3 ماي 2004، ص 395.

52. جورج نهاد أبو جريش وغشان يوسف رشوان، مرجع سبق ذكره، ص 98.

53.مناني فراح، **العقد الالكتروني وسيلة إثبات حديثة في القانون المدني الجزائري**، دار الهدى، الجزائر 2004، ص 188.

54.أحمد شرف الدين، **التوقيع الالكتروني قواعد الإثبات ومتطلبات الأمان في التجارة الالكترونية**، منشورا الحلبي، بيروت 2007، ص 324.

55 جورج نهاد أبو جريش وغشان يوسف رشوان، مرجع سبق ذكره، ص 49. مناني فراح، مرجع سابق، ص189.