التحدي الأمني للتعامل مع البيانات في المصارف الخلوية

عبد الرضا حسن سعود(*)

المستخلص

أصبحت المصارف الخلوية التي جاءت على خلفية اندماج نظم الحوسبة والاتصال ظاهرة مميزة للاقتصاد في المجتمعات المتقدمة، في ضوء ذلك يأتي هذا البحث الذي هو عبارة عن دراسة لمفهوم المصارف الخلوية والتحديات الأمنية التي تواجهها والذي يهدف إلى عرض وتحليل للتحدي الأمني الذي يواجه المصارف التي تعتمد الاتصالات اللاسلكية بشكل عام، فضلا عن بيان الأساليب التي يمكن بتوافرها تحقيق أمن البيانات وإثارة انتباه الجهات التشريعية والقطاع المصرفي في العراق إلى هذا الموضوع في الوقت الحاضر وهو مقبل على حالة بناء متكامل لمصارفه الحكومية والأهلية في ظل مواجهة تحديات العولمة.

ولتحقيق هدف البحث تم اعتماد أنموذجا معيناً، وختم البحث بعدد من النتائج والتوصيات ركزت على أهمية الحماية القانونية لخدمة الهاتف الخلوي كون إن الحماية التقنية تتكفل بها الشركات المصنعة بالدرجة الأساس.

المقدمة

أصبحت المصارف الخلوية التي جاءت على خلفية اندماج نظم الحوسبة ونظم الاتصال ظاهرة مميزة لاقتصاد المجتمعات المتقدمة، وأفرزت طائفة متنوعة من المنافع المتمثلة بتزويد الخدمات المصرفية للزبائن في أي مكان وفي أي وقت، والخدمات المصرفية المزودة عبر الهواتف الخلوية تشمل خدمات المعلوماتية كالاستعلام عن الأرصدة والاطلاع على عروض المصارف وأسعار العملات وفوائدها والاستشارات والنصائح بشأن القروض والتسهيلات وغير ذلك، كما تشمل الخدمات المالية كتحويل النقود من حساب إلى حساب وخدمات الدفع النقدي وفتح الحسابات وإغلاقها وغيرها من الأعمال والخدمات المصرفية. وبالتالي ساهمت في بناء أسواق جديدة وفتح فرص أمام الوحدات الاقتصادية المختلفة، وعلى نفس المنوال تواجه المصارف الخلوية تحديات خطيرة تقع الاحتياطات الأمنية في صدارتها بعد الاعتراف القانوني بالتصرفات والتبادلات التي تتم عبر الهاتف الخلوي، إذ إن أمن التجارة وخصوصية المعلومات المتبادلة عبر هذه الأجهزة تمثل المشكلة الأساسية والرئيسة التي تحظى باهتمام استثنائي من مختلف جهات العمل عبر الوسائط الخلوية، وذلك أن الهاتف الخلوي أضاف مخاطر جديدة في

(*)مدرس مساعد/ قسم المحاسبة/المعهد التقني (ناصرية).

حقل الدخول إلى النظام والالتقاط البعدي للبيانات تسهل معه عملية النفاذ غير المشروع لأنظمة الحاسوب والمواقع المرتبط بها الهاتف الخلوي موضوع الاستخدام.

ولغرض استباق الأحداث كان هذا البحث كمحاولة لإثارة الانتباه إلى هذه التحديات سواء كان على مستوى المصارف العراقية والوحدات الأخرى بشكل عام إذ ينبغي أن تضع ذلك في حساباتها إذا ما أرادت الانتفاع من هذه الممارسة المحاسبية الجديدة أو حتى على مستوى التشريع في البلاد ونحن مقبلون على إصدار قوانين مختلفة لتنظيم الحياة الاقتصادية الجديدة.

أولاً: منهجية البحث

أهمية البحث

تتجلى أهمية البحث من أن العراق مقبل على مايسمى باقتصاد السوق ويعد القطاع المصرفي أحد الركائز الأساسية لهذا الاقتصاد ولا بد له أن يدخل في عالم التقنية الحديثة لكي ينافس المصارف غير العراقية إذا ما دخلت إلى البلاد، فجاء البحث ليلقى الضوء على المصارف الخلوية والتحديات الأمنية تحديداً لكي تؤخذ في الحسبان عند إنشاء البنى التحتية للبلد من جانب أو القواعد التشريعية المتمثلة بالقوانين التي تحكم الأعمال الإلكترونية.

مشكلة البحث

تتمثل مشكلة البحث بعدم اعتماد الأساليب المناسبة في توفير أمن البيانات من الناحية التشريعية وكذلك عدم اعتماد أساليب متطورة من الناحية التقنية لحماية وسائل الاتصال ومراكز استخدامها المتمثلة بالحاسوب في المصارف الخلوية.

هدف البحث

يهدف البحث إلى تحقيق الأتي :

1- عرض وتحليل للتحدي الأمني الذي يواجه التعامل مع بيانات المصارف الخلوية لغرض بناء قاعدة معرفية تساعد قطاع المصارف من استيعاب وفهم هذه الظاهرة العالمية المتقدمة وما يواجهها من تحديات.

2- بيان الأساليب التي يمكن بتوافرها تحقيق أمن البيانات في المصارف الخلوية.

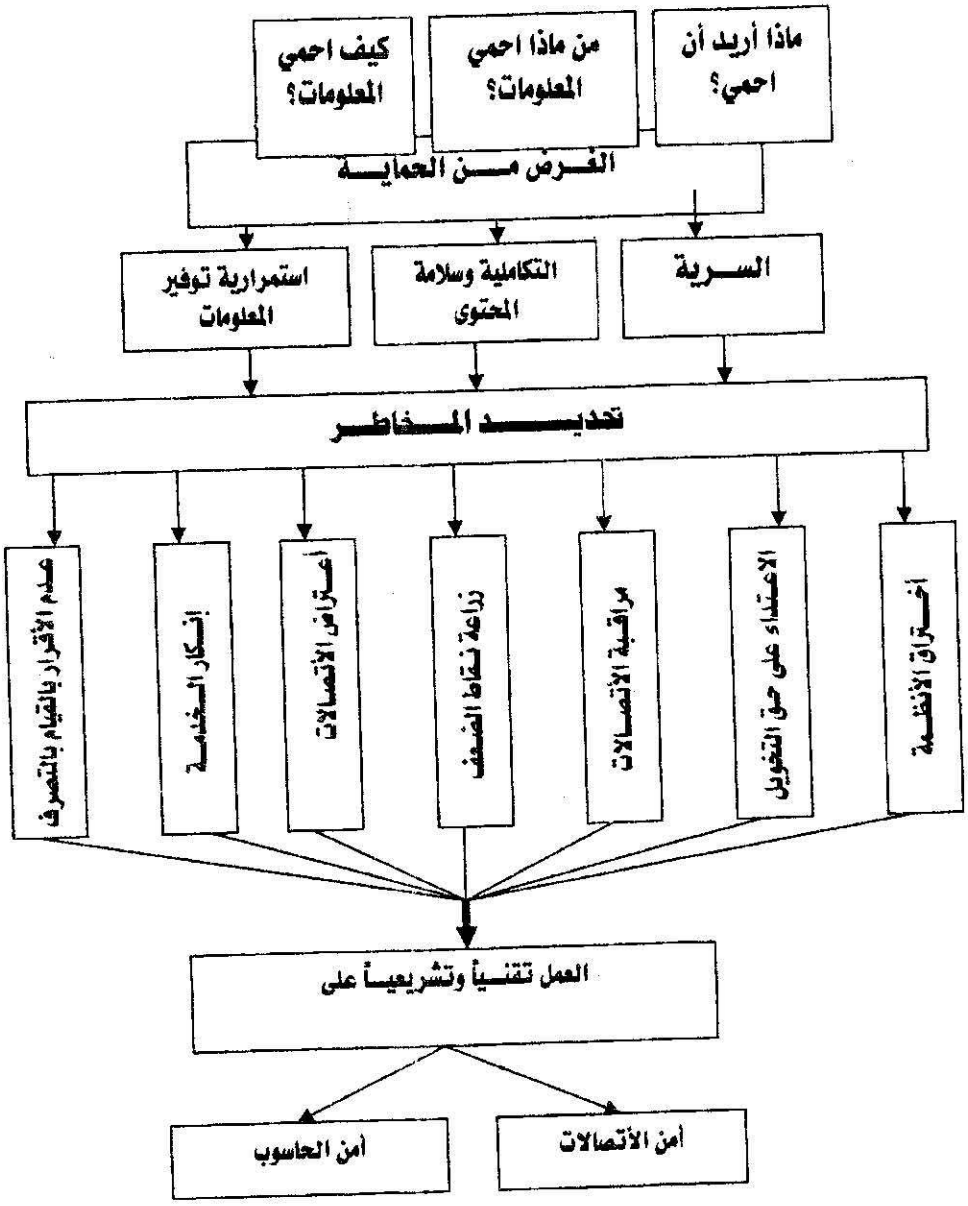
3- إشعار الجهات التشريعية بأهمية اخذ أمن البيانات في المصارف الخلوية في الحسبان وخاصةً في الوقت الحاضر الذي يتميز بانتشار وسائل الاتصال من جانب وكون العراق مقبل على مرحلة بناء متكامل من جانب آخر.

فرضية البحث

يستند البحث على فرضية مفادها:

أن الاهتمام بأساليب أمن البيانات من الناحيتين التقنية والتشريعية يضمن تحقيق سرية وتكاملية البيانات واستمرار توفرها.

أنموذج البحث: وضع الباحث الأنموذج أو المخطط التالي للبحث:



المصدر: من إعداد الباحث

ثانياً: البيانات والمصارف الخلوية Data& Mobile banks

1- البيانات الخلوية ومزايا استخدامها:

البيانات بشكل عام هي المواد الخام التي من خلالها يتم الحصول على المعلومات وهذه الأخيرة تمثل مورداً أساسياً ومهماً كباقي الموجودات الملموسة في المنظمة حيث يعرف نظام المعلومات بأنه مجموعة الأنشطة التي تعمل على جمع ومعالجة وتلخيص البيانات وإيصال المعلومات عبر قنوات الاتصال إلى متخذي القرار.(Romeny et al,2002:20) وأن تقنية المعلومات لها أهمية كبيرة في ظل عصر المعلوماتية ولها أثرها على المعلومة المحاسبية وبالتالي على أداء المنظمة ككل.

نمت في العقدين الماضيين وعلى نحو متسارع الاستخدامات التجارية للوسائط اللاسلكية بعدما كانت منحصرة استخداماتها التجارية في قطاعات النقل البري والجوي والبحري إضافة إلى بعض الاستخدامات المحلية كأجهزة الشرطة مثلاً، ومع تطور أجهزة الاتصالات اللاسلكية واستغلال شبكة الانترنيت تنامي بشكل واسع سوق وسائط الاتصالات اللاسلكية مقابل انخفاض كلفها حيث حدثت قفزات كبيرة في سوق هذه الوسائط إذ من المتوقع أن تنمو عائدات السوق العالمية للمعطيات اللاسلكية نمواً متسارعاً بما يعادل عشرة أضعاف واقعها الحالي وذلك بحسب دراسة لمؤسسة غارتنر غروبز.(Deitel,2001:4) كما إن الدراسات الأخرى أكدت على إن هناك نمو مذهل وغير عادي في سوق استعمال الوسائط اللاسلكية لتبادل بيانات وإجراء الاتصالات وبغض النظر عن كل الدراسات في هذا المجال فأن ما نلمسه اليوم أن هناك تطوراً كبيراً يحدث في مجال استعمال الهاتف الخلوي وظهور مفهوم ما يعرف بالإعمال الخلوية Mobile business(*).

وعليه وفي ضوء ما تقدم فأن الأعمال اللاسلكية هي توظيف وسائط الاتصالات اللاسلكية (الهاتف الخلوي بشكل خاص) في الأنشطة التجارية المختلفة بين مؤسسات الأعمال والزبائن وبين مؤسسات الأعمال فيما بينها بالاعتماد أساسا على فكرة تبادل البيانات في الهواتف الخلوية. وتتمثل الأعمال اللاسلكية ضمن سياق البحث بالأعمال التجارية والمصرفية.

ولاشك إن البيانات الخلوية يمكن تصنيفها بحسب استخدامها إلى تجارية وغير تجارية وما يركز عليه الباحث هنا هو البيانات التجارية، حيث تقوم الفكرة الجوهرية لمختلف

(*)يقول توم فورستر بشأن التطور المذهل لتقنية المعلومات ((لو حدث في تقنية السيارات تقدم مماثل لذلك الذي حدث في تقنية الحاسوب لأمكننا اليوم أن نقتني سيارة رولز رايز بسعر لا يتجاوز دولارين وتساوي قوة محركها قوة سفينة عابرة للمحيطات أو قوة طائرة نفاثة ومعدل استهلاكها للوقود لتر واحد لكل مليون كيلو متر أما حجمها فيساوي 16 بالألف من حجم رأس الدبوس))(فورستر، 68:1989)

الاستخدامات لوسائط الهاتف الخلوي على توفير المعلومات عند طلبها والحاجة إليها وتحويل الهاتف الخلوي إلى بوابة سهلة وميسورة لتقنية المعلومات تتيح الحصول على المعلومات أينما كان المستخدم وفي كل وقت يريد، هذه المعلومات قد تتضمن أحوال الطقس، والسفر والتنقل، والقراءة وتصفح المجلات ، والاطلاع على الأخبار، ومتابعة الأسواق المالية، وحركة الأسهم، الدعاية والإعلانات بشكل تفاعلي، الشراء والبيع والتسوق من مختلف مواقع التجارة والأعمال الإلكترونية، وتنفيذ مختلف الأعمال المصرفية سواء الاستعلامية أو عمليات نقل النقود والدفع وغيرها ، ..... الخ.

بناءً على ذلك فالأجهزة الخلوية واستخدامها في فكرة توفير البيانات تتيح مزايا لعل من أهمها: (جيتس، 1998:63)

a) فاعلية إدارة الوقت وتحديداً في حقل نقل البيانات للزبائن في كل وقت ودون الوقوع في مخاطر التأخير أو الاعتماد على قدرات الموظفين في تنفيذ طلبات التعامل مع الزبائن.
b) تحقيق شخصية الخدمات والاهتمام بشخص العميل إذ تتيح الهواتف الخلوية ربطاً مباشراً بين الخدمة وبين متلقيها وهو ما يوجد شعوراً مميزاً لدى العميل بأنه محط اهتمام في الواقع العملي قد يكون من الصعب ربط الخدمة بالزبون عند تعدد الزبائن لكن في ظل تقنيات الأتمتة فأن نظم ألحواسيب المدمجة وشبكات الهاتف الخلوي تتيح توجيه الاهتمام المباشر للعميل بشخصه وأسمه دون جهد إضافي في بيئة العمل العادية.
c) الإنتاجية وفاعلية الأداء حيث يمكن الاعتماد على البيانات الخلوية في تجاوز معوقات الإنتاج والأداء في أوقات الضغط وأوقات التواجد خارج بيئة العمل.
d) خفض الكلف الإدارية بوجه عام وهذه يعتمد على نطاق التطبيق ومدى صحته ومدى فاعلية الاستفادة من التقنيات الحديثة وهي مسألة تتعلق بإستراتيجيات توظيف التقنية عموماً، لكن من حيث الأصل فأن الاستخدامات الخلوية يتعين أن تتيح توفيراً في الكلف الإدارية وتوفيراً في وسائط إيصال المعلومات للزبون.
e) توفير قاعدة بيانات لخدمة الأعمال في كل وقت وفي كل مكان.
f) سهولة الاستخدام قياساً بالأجهزة التقنية الأخرى التي قد تتطلب دراية للتعامل معها.
g) إلغاء عنصر المكان في تقديم الخدمة بما يتيح تقديم الخدمات في أسواق مفتوحة غير مقيدة بحدود.
h) تطوير قدرات المتابعة والملاحقة ووضع التقارير المتصلة بالعمل وتحديد الاتجاهات سواء ما يتصل بالبيئة الداخلية للمؤسسة أو في العلاقة مع الزبائن والجهات الخارجية.

أذن ومن خلال ما ورد أعلاه من مزايا متعددة لا بد من أن يحظى هذا التطور التقني بالدراسة وأن توضع له كافة التشريعات التي تجعل من استخدامه ممكناً بما يعزز الاستفادة من هذه المزايا.

2)- المصارف الخلوية:

التجارة الإلكترونية E. commerce هي تنفيذ و إدارة الأنشطة التجارية المتعلقة بالبضاعة والخدمات بواسطة تحويل البيانات عبر شبكة الانترنيت أو الأنظمة التقنية الشبيهة.(Koelsch, 1995:320) وتقوم فكرة التجارة عبر الهاتف الخلوي على نفس مفهوم التجارة الإلكترونية من حيث الأصل أي التجارة عن بعد، متضمنة كافة الأنشطة التسويقية والدعاية وكافة أنشطة الشراء والبيع باستخدام الهاتف الخلوي .

وكما هو معروف أن عنصر الزمن في العمل المصرفي من العناصر المهمة إذ إن الزبون لا ينتظر طويلاً لأداء الخدمة له و أساس المنافسة هو تقديم الخدمة في وقت قياسي فضلا عن جودة تلك الخدمة.ولذلك جاء الهاتف الخلوي ليخدم هذا العنصر وبشكل فعال من هنا نشأت فكرة المصارف الخلوية والتي تعتمد أساسا على تزويد الخدمات المصرفية للزبائن في أي مكان وفي أي وقت وتشمل الخدمات المصرفية المزودة عبر الهواتف الخلوية الخدمات المعلوماتية كالاستعلام عن الأرصدة والاطلاع على عروض المصارف وأسعار العملات وفوائدها ومعدلاتها والاستشارات والنصائح بشأن القروض والتسهيلات وغير ذلك من الخدمات كما تشمل الخدمات المالية لتحويل النقود من حساب إلى حساب وخدمات الدفع النقدي وفتح الحسابات وإغلاقها وغيرها من الأعمال والخدمات المصرفية .

وتعد المصارف الخلوية فتحاً جديداً في مجال توظيف البطاقات الذكية تحديداً Smart cardإذ تعد الواسطة الرئيسية لتخزين تطبيقات المصارف الخلوية بأنواعها، سيما أنها تتمتع بقدر من الأمن يفوق الرسائل التقنية الأخرى وتحديداً وسائل الربط والتخزين المفتوحة، وقد أتاحت البطاقات الذكية قدرة تخزين و إدارة التواقيع الإلكترونية ومختلف وسائل التعرف والتثبيت والموثوقية المرتبطة بالأعمال المصرفية وفي العلاقات ما بين المصرف والزبون.(OBrien, 2003:419) منذ انطلاق فكرة الخدمات المصرفية بواسطة الهواتف الخلوية وتوظيف البطاقات الذكية لهذه الغاية جرى تطور مذهل في حقل توظيف الوسائط وبروتوكولات الاتصال وتبادل المعلومات وبروتوكولات ووسائل أمن المعلومات في بيئة مصارف الهواتف الخلوية.ترافق ذلك مع تطور مذهل في حقل البطاقات الذكية، وهي بطاقات أشبه ما تكون بالبطاقات البلاستيكية تحتوي على معالجات أو شرائح رقمية تتيح التخزين وتنفيذ

التطبيقات، وتحتوي على ذاكرة رقمية للاحتفاظ ببرامج التطبيقات، وتمكن البطاقة الذكية من الدخول إلى قواعد البيانات والتفاعل معها كما إنها وفي الوقت الراهن مدمجة بأنظمة عالية من الأمن وتتيح سلامة محتوى البيانات المتبادلة وموثوقية الإطراف على التعامل.

ثالثاً: التحدي الأمني للمصارف الخلوية The security challenge for mobile banks

هناك عاملان أساسيان يمثلان التحدي الأمني في المصارف الخلوية هما:

1)- الخصوصية:

إن الحق في الخصوصية يعرف بحق احترام سرية وخصوصية الأشخاص من أي تدخل مادي أو معنوي، وهو حق عميق الجذور من الوجهة التاريخية، وقد تطور الحق في الخصوصية وحماية البيانات في الستينات والسبعينات نتيجة للتأثر بتقنية المعلومات وبسبب القوى الرقابية المحتملة لأنظمة الحاسوب التي استوجبت وضع قواعد معينة تحكم جمع ومعالجة البيانات الخاصة، وفي هذا الحقل فأن أول معالجة تشريعية في مجال حماية البيانات كان عام 1970 في هيس بألمانيا والذي تبعه سن قانون وطني في السويد عام 1973 ثم الولايات المتحدة عام 1974 ثم ألمانيا على المستوى الفيدرالي عام1977 ثم فرنسا عام 1978.(عرب، 2002:54)

وفي عام 1981 وضع الاتحاد الأوربي اتفاقية حماية الأفراد من مخاطر المعالجة الآلية للبيانات الشخصية، ووضعت كذلك منظمة التعاون الاقتصادي والتنمية دليلا إرشاديا لحماية الخصوصية ونقل البيانات الخاصة، والذي قرر مجموعة قواعد تحكم عمليات المعالجة الإلكترونية للبيانات وهي القواعد تصف البيانات والمعلومات الشخصية على أنها معطيات تتوفر لها الحماية في كل مرحلة من مراحل الجمع والتخزين والمعالجة والنشر، ويمكن تقسيم الخصوصية إلى عدد من المفاهيم المنفصلة لكنها ترتبط معاً في الوقت ذاته وهي:(Levy, 2002:213)

a)-خصوصية المعلومات والتي تتضمن القواعد التي تحكم جمع و إدارة البيانات الخاصة كمعلومات بطاقة الهوية والمعلومات المالية والسجلات الطبية والسجلات الحكومية وهي المحل الذي يتصل عادةً بمفهوم حماية البيانات .

b)-الخصوصية الجسدية أو المادية والتي تتعلق بالحماية الجسدية ضد أي إجراءات ماسة بالنواحي المادية لأجسادهم كفحوص الجينات وفحص المخدرات ....الخ.

c)- خصوصية الاتصالات والتي تغطي سرية وخصوصية المراسلات الهاتفية والبريد بكل أشكاله والاتصالات الخلوية وغيرها من الاتصالات.

d)- الخصوصية الإقليمية والتي تتعلق بالقواعد المنظمة للدخول إلى المنازل وبيئة العمل أو الأماكن العامة والتي تتضمن التفتيش والرقابة الإلكترونية والتوثيق من بطاقة الهوية .

وتمكن تقنية المعلومات الجديدة خزن واسترجاع وتحليل كميات هائلة من البيانات الشخصية التي يتم تجميعها من قبل المؤسسات والدوائر والوكالات الحكومية ومن قبل الشركات الخاصة، ويعود الفضل في هذا إلى مقدرة الحوسبة الرخيصة، واكثر من هذا فأنه يمكن مقارنة المعلومات المخزونة في ملف مؤتمت بمعلومات في قاعدة بيانات أخرى، ويمكن نقلها عبر البلد في ثوان وبتكاليف منخفضة نسبياً، إن هذا بوضوح يكشف إلى أي مدى يمكن تهديد الخصوصية، وتتزايد مخاطر التقنيات الحديثة على حماية الخصوصية، كتقنيات رقابة (كاميرات) الفيديو، وبطاقات الهوية والتعريف الإلكترونية، وقواعد البيانات الشخصية، ووسائل اعتراض ورقابة البريد والاتصالات السلكية واللاسلكية ورقابة بيئة العمل وغيرها.

ولذلك سعت بعض الدول إلى إقرار تشريعات شاملة في حقل حماية البيانات وان هناك الكثير من الدول الأخرى تسعى لوضع قوانين جديدة أو تعديل في قوانينها القائمة لتحقيق حماية البيانات وخصوصاً البيانات الشخصية والأسرار من مخاطر المعالجة الآلية للبيانات، ولعل الهدف الأساسي من وضع مثل هذه القوانين هو الرغبة العامة في تشجيع وتنظيم التجارة الإلكترونية والي يعد من بين موضوعاتها الساخنة مسائل الخصوصية .

وفي دراسة قام بها المركز العربي للقانون والتقنية العالية أظهرت إن قوانين الخصوصية تنطوي على ثلاثة طوائف رئيسية من القواعد:(رستم، 1992: 78)

الأولى: الطائفة المتعلقة بإقرار المبادئ الرئيسية للحق بالخصوصية ونطاق اعتراف الدولة به وكلفته والالتزامات المقررة على الجهات العامة والخاصة في حقل حماية البيانات الشخصية واحترام الخصوصية فيما تمارسه من أنشطة جمع ومعالجة البيانات الشخصية باستخدام التقنية.

الثانية: القواعد التنظيمية والإجرائية والمعايير، وهي تلك القواعد المتعلقة بآليات جمع البيانات ومعالجتها ونقلها وتحدد المعايير التي يتعين على جهات التقنية والاتصالات التقيد بها إلى جانب بحثها في جهات رقابة حماية الخصوصية وتنظيم تشكيلها وعملها وبيان دورها وتحديد مهامها وصلاحيتها، يضاف إليها أيضا القواعد الإجرائية الخاصة التي تطبق بالنسبة للحماية المدنية أو الجزائية المقررة في نطاق القواعد الموضوعية للحماية.

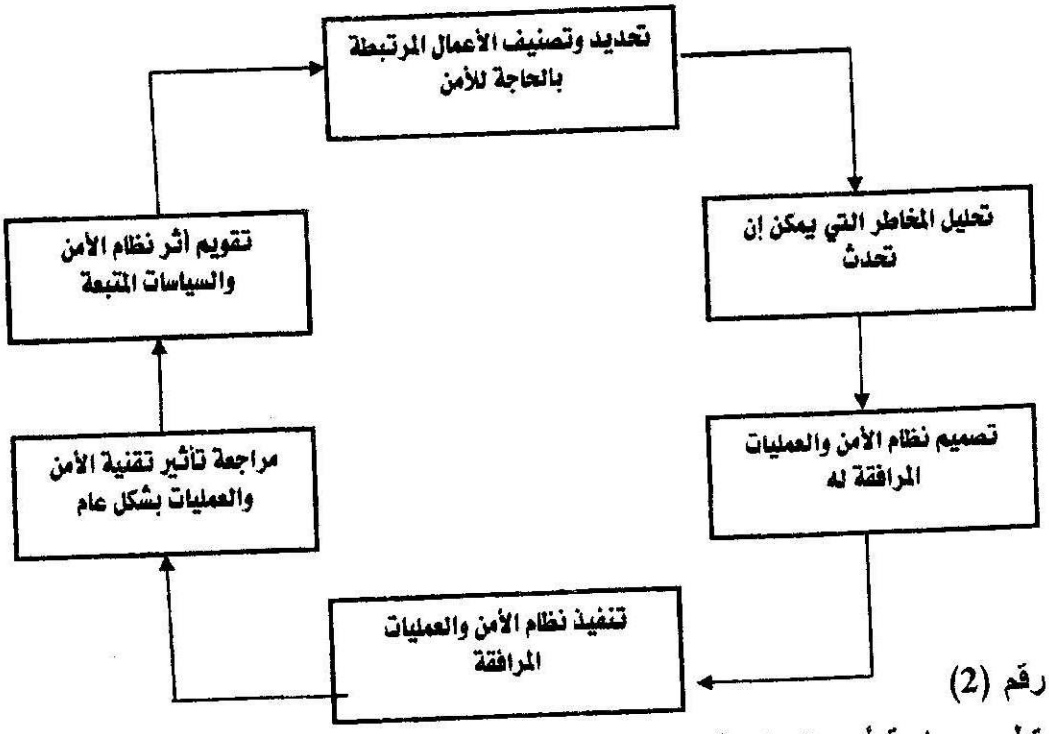
الثالثة: القواعد الموضوعية للحماية المدنية والجنائية، وتشمل نصوص التحريم مع تحديد للأفعال المحرمة وعقوباتها، إضافة لبيان نطاق المسؤولية المدنية وبيان الجهات محل المساءلة وغير ذلك من قواعد موضوعية تتعلق بالحماية القانونية للبيانات الشخصية في كافة مراحل التعامل التقني معها.

وبالعودة إلى خصوصية بيانات وخدمات المصارف الخلوية، فأن حماية هذه الخصوصية وتوفير الثقة لدى الزبون ينطلق من تبني المصرف إستراتيجية واضحة لحماية الخصوصية لدى إدخال هذه الخدمة، تقوم على توفير الحماية التقنية وتأمين الحماية التعاقدية كبديل للحماية التشريعية عند عدم توفرها والعمل في الوقت نفسه على جبهة توفير الحزمة التشريعية المناسبة في هذا الحقل.

2)- مشاكل امن المعلومات:

إن إستراتيجية أمن المعلومات أو سياسة أمن المعلومات هي مجموعة القواعد التي يطبقها الأشخاص لدى التعامل مع التقنية ومع المعلومات داخل المنشأة وتتصل بشؤون الدخول إلى المعلومات والعمل على نظمها و إدارتها . وتهدف إستراتيجية أمن المعلومات إلى تعريف المستخدمين والإداريين بالتزاماتهم وواجباتهم المطلوبة كحماية نظم الكمبيوتر والشبكات وكذلك حماية المعلومات بكافة أشكالها، وفي مراحل إدخالها ومعالجتها وخزنها ونقلها و إعادة استرجاعها، كما تهدف الإستراتيجية إلى تحديد الآليات التي يتم من خلالها تحقيق وتنفيذ الواجبات المحددة على كل من له علاقة بالمعلومات ونظمها وتحديد المسؤولية عند حصول الخطر وتهدف إلى بيان الإجراءات المتبعة لتجاوز التهديدات والمخاطر والتعامل معها والجهات المناط بها القيام بذلك .

وبشكل عام فان تطور نظام أمن المعلومة في المصرف أو في أي وحدة أخرى يمكن أن يمر بدورة متكاملة كما في الشكل التالي:



شكل رقم (2)

دورة تطور سياسة أمن المعلومة

Source: (Coldman & Rawles, 2001: 579)

ويتعين أن تنطلق استراتيجية أمن المعلومات من تحديد المخاطر، أغراض الحماية، مواطن الحماية، أنماط الحماية اللازمة، إجراءات الوقاية من المخاطر، وتتلخص المنطلقات والأسس التي تبنى عليها استراتيجية أمن المعلومات القائمة على الاحتياجات المتباينة لكل منشأة من الإجابة عن تساؤلات ثلاث رئيسية :-

ماذا أريد أن احمي ؟؟ من ماذا احمي المعلومات ؟؟، كيف احمي المعلومات ؟؟ و أما أغراض الحماية فتتمثل بحماية السرية confidentiality والتكاملية وسلامة المحتوى integrity فضلا عن استمرارية المعلومات أو الخدمة Availability وتمتد مناطق أمن المعلومات إلى أمن الاتصالات (ويراد بأمن الاتصالات حماية المعلومات خلال عملية تبادل البيانات من نظام إلى أخر)، وأمن الحاسوب (ويراد به حماية المعلومات داخل النظام بكافة أنواعها وأنماطها كحماية نظام التشغيل وحماية برامج إدارة البيانات وحماية قواعد البيانات بأنواعها المختلفة) ولا يتحقق أمن المعلومات دون توفر الحماية المتكاملة لهذين القطاعين عبر معايير أمنية تكفل توفير هذه الحماية، ومن خلال مستويات أمن متعددة ومختلفة من حيث الطبيعة وذلك كما هو موضح في أنموذج البحث.

وتقوم الإستراتيجية الفاعلة لأمن المصارف الخلوية على تحديد المخاطر بشكل دقيق وشامل وهي مخاطر تتصل بالحاسوب والشبكة وجهاز الهاتف الخلوي نفسه . وابرز هذه المخاطر :ـ

a) اختراق الأنظمة : ويتحقق ذلك بدخول شخص غير مخول بذلك إلى نظام الحاسوب أما عن طريق تظاهر الشخص المخترق بأنه شخص آخر مصرح له بالدخول أو من خلال استغلال نقاط الضعف في النظام كتجاوز إجراءات السيطرة والحماية .

b) الاعتداء على حق التخويل : ويتم من خلال قيام الشخص المخول له استخدام النظام لغرض ما باستخدامه في غير هذا الغرض دون أن يحصل على التخويل بذلك.

c) زراعة نقاط الضعف : وهذه تتحقق عندما يقوم الشخص المخترق بزرع مدخل ما يحقق له الاختراق فيما بعد، أي استخدام برنامج يؤدي غرضا مشروعا في الظاهر لكنه يمكن أن يستخدم في الخفاء للقيام بنشاط غير مشروع .(Donn & B.Parker, 1996 : 65)

d) مراقبة الاتصالات : بدون اختراق نظام الحاسوب للمجني عليه يتمكن الجاني من الحصول على معلومات سرية غالبا ما تكون من المعلومات التي تسهل له مستقبلا اختراق النظام وذلك ببساطة من خلال مراقبة الاتصالات من إحدى نقاط الاتصال أو حلقاتها .

e) اعتراض الاتصالات : قد يعترض الجاني البيانات المنقولة خلال عملية النقل ويجري عليها التعديلات التي تتناسب مع غرض الاعتداء ويشمل اعتراض الاتصالات قيام الجاني لخلق نظام وسيط وهمي بحيث يكون على المستخدم أن يمر من خلاله ويزود النظام بمعلومات حساسة بشكل طوعي .

f) إنكار الخدمة : ويتم ذلك من خلال القيام بأنشطة تمنع المستخدم الشرعي من الوصول إلى المعلومات أو الحصول على الخدمة .

g) عدم الإقرار بالقيام بالتصرف : ويتمثل هذا الخطر في عدم إقرار الشخص المرسل اليه أو المرسل بالتصرف الذي صدر عنه، كأن ينكر أنه ليس هو شخصيا الذي قام بإرسال طلب الشراء عبر الانترنيت .

رابعاً: عناصر حماية الهاتف الخلوي في التبادلات المصرفية:

1- عناصر الحماية التقنية.

مع تزايد القيمة الاقتصادية والمالية للمعلومات، وشيوع وتنامي التطبيقات العملية لفكرة رأس المال الفكري والاقتصاد القائم على المعرفة والاقتصاد الرقمي، وجب العمل على توفر الحماية التقنية لنظم المعلومات بوجه عام وهو ما أدى إلى ابتكار وسائل تقنية متنامية كجدران

النار وكلمات السر ووسائل التصريف البايلوجية والتشفير وغيرها لضمان حماية تبادل المعلومات بشكل صحيح والحفاظ على السرية ، إلا أن الحماية التقنية ليست كافية لضمان حماية المعلومات ونظمها وتطبيقاتها، عوضاً عن أنها لم تؤدي إلى توفير ثقة واسعة في نظم التقنية لدى المستخدمين الذين تسود عندهم قناعة إن نظم الحاسوب والانترنيت ووسائل الاتصال اللاسلكي ليست آمنة بقدر الوسائل التقليدية للأعمال القائمة على الورق والدليل الكتابي أو المادي، لهذا كان لزاماً أن تتحرك النظم القانونية لضمان توفير حماية المعلومات

وإذا ما أردنا تصنيف خدمات الأمن في ضوء العناصر الرئيسية في مجال المعلومات التي تستهدف حمايتها فيمكن أن تكون في خمسة أنواع هي :(موسكوف وسيمكن ، 2002 : 576)

a) **خدمات حماية التعريف :**

هذه الخدمات تهدف إلى التثبت من الهوية وتحديدا عندما يقوم شخص ما بالتعريف عن نفسه فان هذه الخدمات تهدف إلى التثبت من انه هو الشخص نفسه ولهذا فأن التعريف يعد الوسائل التي تحمي من أنشطة التخفي والتنكر ومن هنا فأن هناك نوعان من خدمات التعريف الأول تعريف الشخصية وأشهر وسائلها كلمات السر وثانيها التعريف بأصل المعلومات كالتثبت من أصل الرسالة .

b) **خدمات السيطرة على الدخول :**

هذه الخدمات تستخدم للحماية ضد الدخول غير المشروع إلى مصادر الأنظمة والاتصالات والمعلومات ويشمل مفهوم الدخول غير المصرح به لإغراض خدمات الأمن جملة من الأعمال غير المصرح بها كالاستخدام والإفشاء والتعديل والإتلاف وإصدار التعليمات والأوامر . ولهذا فان خدمات التحكم بالدخول تعد الوسائل الأولية لتحقيق التخويل والتثبت منه .

c) **خدمات السرية :**

هذه الخدمات تحمي المعلومات من الإفشاء للجهات غير المصرح لها بالحصول عليها، والسرية تعني بشكل عام إخفاء المعلومات من خلال تشفيرها أو من خلال وسائل أخرى كمنع التعرف على حجمها أو مقدارها أو الجهة المرسلة أليها .

d) **خدمات حماية التكاملية وسلامة المحتوى :**

هذه الخدمات تهدف إلى حماية مخاطر تغيير البيانات خلال عمليات إدخالها أو معالجتها أو نقلها وعملية التغيير تعني بمفهوم الأمن هنا الإلغاء أو التحوير أو إعادة تسجيل جزء منها أو

غير ذلك وتهدف هذه الوسائل أيضا إلى الحماية من أنشطة تدمير المعطيات بشكل كامل أو إلغاءها دون تخويل.

e) **خدمات منع الإنكار:**

وهذه الخدمات تهدف إلى منع الجهة التي قامت بالتصرف من إنكار حصول نقل البيانات أو النشاط من قبلها.

وتعد هذه الأنواع الخمس المناطق الأساسية لحماية المعلومات .

وبشكل عام فأن مختلف وسائل الحماية(التقنية والقانونية) تهدف إلى تأمين الحماية في المواضيع التالية والتي تمثل في الوقت ذاته عناصر النظام الأمني للمعلومات المتبادلة بواسطة الهواتف الخلوية: (Goldman & Rawles, 2001:429)

a) القدرة على إثبات شخصية الطرف الآخر على الشبكة وبنفس الوقت إثبات شخصية الموقع للمستخدم.

b) الخصوصية أو حماية بيانات المستخدم من الإفشاء والاطلاع دون أذن أو تخويل.

c) الصلاحيات وتحديد مناطق الاستخدام المسموحة لكل مستخدم وأوقاته.

d) تكاملية أو سلامة المحتوى وتتصل بالتأكد من إن المعلومة التي أرسلت هي نفسها التي تم تلقيها من الطرف الأخر .

e) عدم الإنكار إذ لا يكفي فقط إثبات شخصية المستخدم أو الموقع بل يتعين ضمان عدم إنكار منفذ التصرف صدور التصرف عنه.

f) استمرارية توفر المعلومات أو الخدمة إذ لا يكفي الوجود وتقديم الخدمة الإلكترونية ووجود النظام الإلكتروني ويتعين ضمان استمرار الوجود وحماية النظام من أنشطة التعطيل.

2- عناصر الحماية التشريعية:

إن اخطر ما يواجه نظم حماية المعلومات وفعالية الأدوات التشريعية لتنظيم استخدامها وتطبيقاتها وصورها والمعالجات للتحديات القانونية المتعلقة بتقنية المعلومات هو الحاجة إلى حزمة متكاملة من التشريعات في حقل تقنية المعلومات تمتد لتغطية أربعة عناصر أساسية:(رستم، 1992 : 112)

a) الاعتراف القانوني بالمعلومات ووسائل حمايتها في النظام القانوني.

b) التنظيم الملائم لوسائل التقنية ومعاييرها ومواصفاتها.

c) الاعتراف القانوني بصلاحية الوسائل الإلكترونية في بيئة الأعمال والخدمات والاستثمار.

d) الاعتراف القانوني بمصالح المستهلك والمستخدم وتوفير الحماية القانونية من عيوب ومخاطر التقنية وتطبيقاتها.

وهذه العناصر الأربعة تمثل الإطار القانوني الذي تتدرج في نطاقه مختلف تشريعات تقنية المعلومات، بحيث لا تكون حزمة التشريع فاعلة أو كافية ما لم تضمن حماية المعلومات ذاتها من أنشطة الاعتداء عليها، وحماية المستخدم من مخاطر التقنية وتختلف المواصفات وما قد يتعرض له من أنشطة جرمية، وتوفير بيئة ملائمة للأعمال الإلكترونية بمختلف تطبيقاتها من خلال الاعتراف بالوسائل الإلكترونية بمختلف أنواعها للتعاقد والإثبات وتوفير معايير سلامة النشاط التجاري والاستثماري في البيئة الافتراضية للأعمال اللاسلكية بذات القدر الذي تحظى به في بيئة العالم الحقيقي أو الورقي.

خامساً: الاستنتاجات والتوصيات

الاستنتاجات

من خلال ما ورد في البحث يمكن للباحث أن يضع الاستنتاجات التالية:

1- إن الحماية القانونية لخدمة الهاتف الخلوي المصرفية تعادل أو تفوق من حيث الأهمية البنى التحتية وخطط الاستثمار لهذه الخدمة.

2- يعد أمن الاتصالات وأمن الحاسوب العنصران الأساسيان اللذان يحكمان العملية الأمنية لخدمة الهاتف الخلوي المصرفية.

3- افتقار العراق إلى تشريعات تحكم العملية الأمنية للاتصالات اللاسلكية بشكل عام والتجارية منها بشكل خاص رغم انتشار خدمة الهاتف الخلوي وشبكة الانترنيت منذ ما يقارب الثلاث سنوات تقريباً.

التوصيات

في ضوء الاستنتاجات السابقة يوصي الباحث بالآتي:

1- يوصي الباحث أن تؤخذ في الحسبان التشريعات القانونية الخاصة بتنظيم الأعمال التجارية من خلال الاتصالات اللاسلكية لا سيما ونحن مقبلون على حالة بناء متكامل للتشريعات القانونية من جانب، ومن جانب آخر مقبلون على تبني سياسة الاقتصاد المفتوح وفتح الاستثمار أمام القطاع الخاص العراقي والعربي والأجنبي.

2- إذا ما أردنا أن نطوع خدمة الهاتف الخلوي في عالم الأعمال وتحديداً في النشاط المصرفي يجب أن ينصب الاهتمام على الحماية القانونية رغم أهمية الحماية التقنية إلا إن هذه الأخيرة تتطور على المستوى العالمي وما يصلح منها في أي مكان في العالم يصلح للعراق على عكس الحماية القانونية والتي يجب أن تتماشى والواقع العراقي تحديداً.

3- على القطاع المصرفي العراقي أن يحث الخطى للحاق بالتطور التقني الهائل للعمل المصرفي لكي يكون قادراً على الصمود والبقاء في السوق وان لا يكون مجرد دائرة تمول مركزياً وغير هادفة إلى الربح وفي مقدمة ما يجب عمله إدخال الملاكات المصرفية المختلفة بدورات تدريبية وتأهيل على التطورات التقنية المتسارعة.

مراجع البحث

أولاً. الكتب العربية

1- جيتس، بيل، المعلوماتية بعد الانترنيت، ترجمة ونشر دار المعرفة، الكويت ، 1998.

2- رستم، هشام محمد فريد، قانون العقوبات ومخاطر تقنية المعلومات، الطبعة الأولى، مكتبة الآلات الحديثة، أسيوط، 1992.

3- عرب، يونس، الخصوصية وحماية البيانات في العصر الرقمي، منشورات اتحاد المصارف العربية ، 2002.

4- فوريستر، توم ، مجتمع التقنية العالية- قصة ثورة تقنية المعلومات، الطبعة الأولى، ترجمة ونشر مركز الكتاب الأردني، عمان، 1989.

5- موسكوف ، ستيفن وسيكمن ، مارك، نظم المعلومات المحاسبية لاتخاذ القرارات، ترجمة كمال الدين سعيد، دار المريخ، الرياض، 2002.

ثانياً. الكتب الأجنبية

1 - Deitel , H.M. , & Steinbuhler , K. , e - Business and e - commerce , prentice - Hall , Inc. ,New Jersey ,2002 .

2- Donn , B. Parker , Crime by computer , second edition , charles , scribners sons , New York , 1996.

3- Flynn D., Information systems requierements: Detrmination and analysis, second edition, McGraw - Hill, 2000.

4 - Goldman , James E. & Rawles , philip T. , Applied data communication , Third edition , John wiley & sons Inc. , USA ,2001.

5- Koelsch, Frank, The infomedia revolution, McGraw - Hill Ryerson, Toronto / Canada, 1995.

6- Levy, Steven, Saving privacy in the digital age, McGraw - Hill, Co. Inc., USA, 2001.

7-OBrien , James A. , Introduction to information systems , 11th edition , McGraw - Hill , Co. Inc. , USA, 2003.

8-Romeny Marshall B., Steinbert Paul , Accounting Information Systems, Idea group publishing , 2002, p.20.