« جرائم بطاقة الدفع الإلكتروني عبر شبكة الانترنت »

إعداد المستشار الدكتور/ امجد حمدان الجهني

قاضي محكمة أبو ظبي الابتدائية

المقدمة:

تحديد ماهية الاستخدام غير المشروع لبطاقة الدفع الإلكتروني عبر الانترنت:

لم يكن هناك محاولات فقهية جادة لوضع تعريف للاستخدام غير المشروع لبطاقة الدفع الإلكتروني، والسبب في ذلك أنّ الاستخدام غير المشروع عملية معقدة، ومركبة لا تُعرف إلا من خلال بيان نقيضها، وهو الاستخدام المشروع للبطاقة، بحيث إن ما يخرج عن هذا الاستخدام يكون غير مشروع.

يضع بعض الفقه(١) تعريفاً للاستخدام غير المشروع لبطاقة الدفع الإلكتروني، بأنه "عندما يخل الحامل بشروط عقد إصدار البطاقة، بما يؤدي إلى فسخ هذا العقد، أو قفل الحساب الذي تقوم البطاقة بتشغيله، حيث يسأل الحامل جنائياً لمجرد امتناعه عن رد البطاقة، أو استمراره في استخدامها بعد إلغائها من البنك المُصدر لها، أو استمراره في استخدامها بعد انتهاء مدة صلاحيتها".

---

(١) أبو الوفا محمد أبو الوفا إبراهيم: المسئولية الجنائية عن الاستخدام غير المشروع لبطاقة الائتمان، ورقة عمل مقدمة في مؤتمَّر الأعمال المصرفية الإلكترونية بين الشريعة والقانون من ٩ – ١١ ربيع أول ١٤٢٤هـ. الموافق ١٠ – ١٢ أيار ٢٠٠٣م، كلية الشريعة والقانون/جامعة الإمارات العربية المتحدة وغرفة تجارة وصناعة دبي، دولة الإمارات، المجلد الخامس، ص٢٠٧٠.

وإنني أعيب على هذا التعريف محدوديته حيث إنه يتناول حالة واحدة من حالات الاستخدام غير المشروع لبطاقة الدفع الإلكتروني، وهو حالة الاستخدام غير المشروع من قبل الحامل، ولم يتناول الحالات التي تتم من قبل التاجر، والغير، والمصدر في بعض الأحيان.

لذا فإنّني أرى أنه لا يمكن وضع تعريف للاستخدام غير المشروع لبطاقة الدفع الإلكتروني وتحديد ماهيته تحديداً دقيقاً، حيث إن الاستخدام غير المشروع هو عبارة عن حالة، أو حالات تختلف باختلاف الشخص أو الجهة التي قامت بمزاولته، كما أنّ هذه الحالات تتطور بتطور وسائل حماية البطاقة، فقد تظهر حالات للاستخدام غير المشروع في المستقبل، غير معروفة في الوقت الحاضر، كما أنّ الفروق بين الاستخدام غير المشروع، أو بينها وبين الأخطاء الفنية غير المقصودة، أو بينها وبين الحصول على البطاقة بطرق غير مشروعة هي فروق دقيقة يصعب تمييزها، بحيث يثور التساؤل: أي منها يُعدّ استخداماً غير مشروع لبطاقة الدفع الإلكتروني؟

ويمكن القول أن الاستخدام المشروع للبطاقة هو: الاستخدام الذي يتمّ بواسطة الحامل الشرعي والبطاقة صحيحة[٢] وفي الغرض المخصص لها، وفي حدود سقفها، وبالتالي فإنّ شروط الاستخدام المشروع لبطاقة الدفع الإلكتروني يمكن لي أن أجملها بما يلي:

---

(٢) كيلاني عبد الراضي محمود، النظام القانوني لبطاقات الوفاء والضمان، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، القاهرة، جمهورية مصر العربية ١٩٩٦، ص٧٣٩.

١. أن يكون استخدام البطاقة من قبل حاملها الشرعي(٣).
٢. أن تكون بطاقة الدفع الإلكتروني صحيحة، وغير مزورة أو تمّ التلاعب بها.
٣. أن يكون استخدام بطاقة الدفع الإلكتروني خلال مدة صلاحيتها، وسريانها وفي حدود سقفها.
٤. أن يكون استخدام بطاقة الدفع الإلكتروني في حدود الوظيفة التي أنشئت من أجلها، وهو تسهيل عملية الشراء.

وأي استخدام لبطاقة الدفع الإلكتروني لا تتوافر فيه الشروط السابقة يخرج به من دائرة المشروعية ويضعه في دائرة اللامشروعية، وتقوم بالتالي مسئولية الشخص الذي قام بهذا الاستخدام سواء الحامل أو المُصدر، أو التاجر، أو الغير.

(٣) وهذا ما نصّت عليه جميع عقود استخدام بطاقة الدفع الإلكتروني نذكر منها على سبيل المثال لا الحصر: المادة (٧) من الشروط والأحكام العامة الخاصة بحملة بطاقات الفيزا الصادرة عن بنك الإسكان للتجارة والتمّويل. والمادة (٦) من شروط إصدار، واستخدام بطاقة فيزا الصادرة عن بنك المؤسسة العربية المصرفية. والمادة (٢) من إتفاقية شروط استعمال بطاقة ناشونال اكسبرس.

المبحث الأول

طرق ووسائل الاستخدام غير المشروع

لبطاقة الدفع الإلكتروني عبر الإنترنت

تحولت معظم بطاقات الوفاء العالمية المعروفة، أمثال فيزا Visa، وماستر كارد (Master Card)، وأمريكان اكسبرس[٤] American Express))، إلى وسيلة دفع إلكترونية فِعلية عن بعد، يمنح حاملها رقماً سرياً أو رمزاً سرياً يستخدمه في عملية الدفع، أو التحويل أو في سحب الأموال، ويسمى استخدام الرمز السري للدفع بالبطاقة (بالتوقيع الإلكتروني)، لكن يستتبع ذلك نشوء مخاطر متعلقة بقضية القرصنة المعلوماتية المحتملة للأرقام السرية التي تتجول داخل شبكة الإنترنت[٥]، وسوف أتعرض لآليات الدفع بالبطاقة عبر الإنترنت ووسائل قرصنتها من خلال المطلبين التاليين:

المطلب الأول: آلية الدفع بالبطاقة عبر الإنترنت.

---

(٤) أصدرت أميركيان اكسبرس في عام ٢٠٠٣ بطاقة جديدة باسم الزرقاء (Blue) تحوي على رقيقة إلكترونية، وتتمَّتع بضمان الحماية ضد الإحتيال عبر الإنترنت، بحيث إن حاملها لن يتحمل مسئولية أي تعاملات تمَّت باستخدام البطاقة، أو رقمها دون أن يكون هناك تفويضاً منه، انظر: WWW. American express. Com. Bh

(٥) طوني ميشال عيسى: التنظيم القانوني لشبكة الإنترنت، دراسة مقارنة في ضوء القوانين الوضعية والاتفاقيات الدولية، المنشورات الحقوقية، صادر، بيروت، لبنان، الطبعة الأولى، ٢٠٠١، ص٢٩٩ و٣٠٠.

تتم عملية الدفع بالبطاقة المصرفية عبر الإنترنت(٦)، بإرسال رقم البطاقة من صاحبها عبر الشبكة، بهدف تحويل مبلغ من المال من حساب المشتري إلى حساب التاجر (الموقع التجاري على شبكة الإنترنت(٧)) وذلك ثمناً لسلعة أو خدمة.

---

(٦) حسين إبراهيم القضماني: البطاقة المصرفية والإنترنت، دراسة حول الوضعيتين التقنية والقانونية، مجلة اتحاد المصارف العربية، بيروت، لبنان، الطبعة الأولى، ٢٠٠٢. ص٤٤ وما بعدها.

(٧) من أهم المواقع التجارية على شبكة الإنترنت:

أولاً – المواقع العالمية:

- موقع Amazon. Com

لا نبالغ إذا قلنا بأن موقع Amazon. Com هو من أشهر المواقع في مجال التجارة الإلكترونية الذي يطبق نظام الشراء بالبطاقة، وقد بدأ موقع Amazon. Com رحلته التطويرية عام ١٩٩٤ حتى أضحى اكبر البائعين على الإنترنت في العالم، وهو اليوم يقوم بعرض الملايين من السلع على زبائنه البالغين ١٧ مليوناً، والقاطنين في ١٦٠ دولة في العالم، ويمكن كذلك اعتبار Amazon. Com من أكبر المروجين للمزاد بطريقة الـ(on – line). وتجدر الإشارة إلى أن العمل الذي كان يؤديه هذا الموقع في البدء كان مقتصراً على بيع الكتب عبر البريد الإلكتروني، لكنه دخل عالم بيع الأقراص المدمجة (CD) والصورية (DVD) والبطاقات الإلكترونية والبرامج وغيرها، والحق أن لائحة منتجات amazon. Com تزداد حجماً يوماً بعد أخر، حيث يمكنك بسهولة التبضع عبر هذا الموقع واختيار السلعة التي تناسبك من بين ملايين السلع المعروضة فيه.

- موقع (ياهو).. تجارة: http: //shopping. Yahoo. Com

ياهو للتسوق تجمع الآلاف من التجارات المتعددة في مكان واحد حيث تمتلك ياهو أكثر من ٩٠٠٠ مركزاً تجارياً على هذه الشبكة وهدفها أن تصبح الأكبر عالمياً لصفقات الويب إلى جانب إضافة تجارة جديدة كل يوم:

إن التسوق المعروف سهل لكن ياهو تجعله أكثر راحة، ومثل جميع أقسام ياهو، قسم ياهو للتسوق منظم إلى فئات مختلفة حسب السلعة ولديه وصلات تمدك بالمحتويات، ويوجد بها أداة بحث تساعدك على إيجاد المواد التي تريد شراءها.

- موقع www.ebay.com:

أسس هذا الموقع العالمي للتجارة الإلكترونية في تشرين الثاني من عام ١٩٩٥ لبيع سلع وخدمات متنوعة، واليوم يشترك عشرات الملايين من المستهلكين من مختلف أنحاء العالم للتبضع من هذا الموقع ويقضي عدداً كبيراً منهم اوقاتاً كبيرة في التجول بين متاجر ebay الكثيرة؛ ويعرض الموقع أكثر من ١٦ مليون سلعة. =

ثانياً – المواقع العربية:

- تجاري. كوم: www.tejari.com :

من البوابات العربية الرائدة على شبكة الإنترنت تعمل في مجال B2B، فهي موجهة لخدمة قطاعات الأعمال حيث تتمَّ من خلالها عرض منتجات أكثر من ٧٠ شركة تمثّل ٦٠ ألف منتج في مختلف المجالات، وهي شركة أنشئت بناء على توجيهات سمو الشيخ محمد بن راشد آل مكتوم، وهي جزء من التوجه نحو الحكومة الإلكترونية بدبي فيتيح تجاري دوت كوم فرصة فريدة للعملاء لاستغلال كامل مزايا إبرام الصفقات التجارية بين الشركات بدءا من صفقات الشراء الفوري وانتهاء بالمناقصات والتوريدات ويسمح تجاري دوت كوم للمصنعين والموردين بعرض منتجاتهم وخدماتهم في السوق الإلكترونية وأن الهدف من هذه البوابة الإلكترونية: هو تشجيع التجارة الإلكترونية العربية.

- سوق عجيب: hpp://shop.ajeeb.com/shop:

يحتوي على مجموعة كبيرة ومتميَّزة من المتاجر والمحلات على مختلف أنواعها: التقليدية والشهيرة، الصغيرة والكبيرة والبائعين المشهورين، وهناك طريقتان للتسوق: إحداهما أن تستخدم صندوق البحث الموجود أعلى سوق عجيب، وذلك بإدخال اسم المنتج، وستظهر لك قائمة للمنتجات المناسبة، والطريقة الأخرى أن تتصفح خلال مجموعات متاجر عجيب وان تقوم باختيار مختلف المنتجات التي تعجبك.

- موقع uaemall.com:

حصل هذا الموقع التجاري على جوائز best e- shopping site وغيرها، ويعد هذا السوق من أوائل الأسواق الإلكترونية بدولة الإمارات العربية المتحدة ويغطي المنطقة العربية بالتنسيق مع شركات من جميع أنحاء العالم من جنوب شرق آسيا والشرق الأدنى والشرق الأوسط وأوروبا وأمريكا، وله فروع عديدة في منطقة الخليج والشرق الأوسط وهو موقع ناجح ويلاقي إقبالا كبيراً من المستهلكين لتنوع متاجره بالسلع المختلفة ومعقولية أسعاره.

- صدف كوم: www.sadaaf.com :

فعند دخول المستهلك إلى الموقع المتخصص في بيع السلع على شبكة الإنترنت، تظهر أمامه على الشاشة المعروضات المتوافرة بالأسماء أو بالصور، ويكون السعر مدوناً بجانب الاسم أو الصورة، ولدى اختيار المستهلك لأحد هذه السلع يضغط بواسطة (الفأرة) على الرسم أو الصورة، أو على مفردة (Add To Shopping Cart)، أو بالعربية (أضف إلى عربة التسوق) المجاور للرسم ثم يظهر له على الشاشة رسم السلعة مع مواصفاتها، وعند تصميم المستهلك على الشراء يضغط على خانة تحتوي على كلمة تفيد (الشراء)، مثلاً (حسابي)، أو بالإنجليزية (My Account) فيرسل إليه برنامج التاجر نموذجاً، لمعرفة ما إذا كان المستهلك زبوناً جديداً أم أنه سبق له واشترى من الموقع[1].

بعد ملء النموذج الذي يحتوي عادة على خانة للبريد الإلكتروني، وخانة لكلمة المرور (Password)، وخانة كتب عليها (Enter)، وعند الضغط على خانة (Enter)، تظهر أمامنا على الشاشة نموذجاً ثالثاً مفصلاً لكتابة الاسم الكامل،

وهو أول موقع سوري لبناني للتجارة الإلكترونية مختص بتسويق المنتجات والخدمات السورية واللبنانية مباشرة عبر الإنترنت.

ويتألف هذا الموقع من أقسام عدة تشمل الصناعة والتجارة والزراعة والسياحة والخدمات بالإضافة إلى قسم عرض الكتيبات الخاصة بالمنتجات (الكتالوجات).

ويهدف موقع صدف إلى فتح أسواق جديدة أمام قطاع الأعمال في سوريا ولبنان بغية تصريف منتجاتهم كما يهدف إلى تلبية احتياجات المستهلكين وتقديم خدمات من شأنها تسهيل عملية الحصول على كل ما يرغبون به من سلع وخدمات مختلفة.

انظر: عبد الحق حميش، حماية المستهلك الإلكتروني، ورقة عمل مقدمة إلى مؤتمَّر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، دولة الإمارات المتحدة، المشار إليه سابقاً، ص(١٢٨٢ – ١٢٨٤).

(١) وهذا ما يظهر من النموذج المرسل.

والعنوان الكامل والبريد الإلكتروني، ورقم الهاتف، وخانة أسفل الشاشة يكتب عليها بالإنجليزية عادة Submit)).

وبعد ملء النموذج بالطريقة المطلوبة وإرسالها يعود البرنامج بنموذج رابع، وبعد كتابة الطلبات ومواصفات الحساب والضغط على خانة (Submit) تتم العملية المصرفية إلكترونيا خلال ثوانٍ معدودة التي تؤدي إلى إتمام عملية الدفع، وقد لا تؤدي.

إذن عملية استخدام بطاقة الدفع الإلكتروني عبر شبكة الإنترنت تمر بثلاث مراحل:

المرحلة الأولى: مرحلة البيع (Sale):

بعد ملء النماذج والضغط على خانة (Submit)، من قبل صاحب البطاقة، يرسل البرنامج إلى الزبون نموذجاً خامساً يرمي إلى تحديد السلعة المطلوبة وتسجيل رقم البطاقة ونوعها وصلاحيتها، ولدى ضغط الزبون مرة أخرى على خانة (Submit) ينتقل النموذج إلكترونياً إلى الصندوق الإلكتروني للتاجر، ويتمّ ذلك في اللحظة نفسها.

المرحلة الثانية: مرحلة الاستئذان بالدفع (Authorization):

إن تأهيل برنامج التاجر (Logical Merchant)، لتسيير عملية الدفع يجعله يرسل النموذج إلكترونياً إلى مصرف التاجر الذي يسمى البنك المحصل (Acquiring Bank)، حيث يتمّ تحويل نموذج الشراء إلكترونياً إلى بنك صاحب البطاقة الذي يسمى البنك المُصدر من خلال إحدى الشبكتين (Visa net) أو (Bank net) التابعتين لشركتي (Visa & Master Card)، المغلقتين والآمنتين، وبوصول

النموذج إلى (Server) المصرف المُصدر (Issuing Bank)، يتمّ تحديد ما إذا كان صاحب البطاقة ذا ملاءة مالية أم لا.

وفي حالة انتهاء صلاحية البطاقة، أو عند عدم ملاءة صاحبها، أو أي خطأ يجعل عملية الدفع صعبة، يعود النموذج إلكترونياً، مرفقاً بإشارة عدم التفويض مع بيان سببه، على الخط الإلكتروني، الذي وردت من خلاله، وفي هذه الحالة تنتهي مرحلة التفويض سلبياً؛ أما في حالة ملاءة صاحب البطاقة فتبتدئ المرحلة الثالثة.

المرحلة الثالثة: مرحلة الإبراء (Settlement):

يعود النموذج من خلال الخط الإلكتروني نفسه إلى صاحب البطاقة، يصاحبها إشارة مفادها أن عملية الدفع قد أنجزت حيث يحصل إلكترونياً تحويل المال من حساب صاحب البطاقة لدى البنك المُصدر للبطاقة إلى حساب التاجر في بنكه الذي يسمى البنك المحصل، وهكذا تنتهي عملية الدفع بالبطاقة عبر الإنترنت مع التذكير بأن المراحل الثلاث لا تستغرق سوى بضع ثوان.

لكن عمليات الدفع بالبطاقة المصرفية عبر الإنترنت، اصطدمت بعقبات كثيرة ذات الصلة بأمن عمليات الدفع وسلامتها، فعمدت مجموعات من الشركات العالمية، إلى إنشاء أنظمة تكنولوجية معلوماتية تؤمن سرية انتقال أرقام البطاقات، وسلامة عمليات الدفع عبر الإنترنت، ومن بين هذه الأنظمة، ما أعلنت عنه شركتا فيزا Visa وماستر كارد MasterCard بتاريخ ١٩٩٦/٢/١، في بيان مشترك عن وضع نموذج تقني موحد في موضوع الدفع ببطاقة الدفع الإلكتروني عبر شبكة الإنترنت، سمي نظام (الصفقات الإلكترونية الآمنة Secure

Electronics Transactions Protocol) أو SET[٨]، من أجل جعل التبادل التجاري والدفع عبر الإنترنت آمناً، وذلك بعد أن سبق لكل من هاتين الشركتين أن أعدتا نظاماً مستقلاً خاصاً بهما وبمواصفات مختلفة[٩]، بعد ذلك انضمت إلى هذا المشروع شركات أمريكية أخرى[٣] ومن ثم عدلت الشركة الفرنسية (Euro pay France) في بعض التقنيات المعتمدة لدى(SET) وأطلقته تحت شعار معدل باسم (C – SET).

بالإضافة إلى ذلك، عمدت كبرى الشركات المعلوماتية في العالم، أمثال ميكروسوفت (Microsoft) ونتسكايب (Netscape) وغيرهما، إلى تجهيز البرامج المتصفحة التي ينتجونها بوظائف مماثلة، تعمل وفق بروتوكول معروف باسم (Secure Socket Layers)(SSL) أي طبقة المقاييس الآمنة، من شأنها أن تسمح بإبرام صفقات أو إتمام عمليات دفع آمنة عن بعد، وقد بدأت الإصدارات الأخيرة لبرنامجي نتسكايب(Netscape Communicator) وبرنامج اكسبلورر(Internet Explorer Browser)الأكثر شهرة اليوم في مجال تصفح مواقع الويب في شبكة الإنترنت، تتضمن وظيفة التوقيع الإلكتروني التي تسمح بتوفير الأمن اللازم للبيانات،

---

(٨) يرتكز هذا النظام على استخدام آمن لبطاقات الدفع الاعتيادية يقوم على مبدأ تشفير الأرقام السرية وقت تبادلها عن بعد، ويقيم علاقة ثلاثية بين التاجر وبين شركة خدمات الوساطة وبين الهيئة التي تتولى عملية الدفع. ونشير إلى ان انتشار استخدام بطاقات فيزا وماستر كارد على المستوى العالمي هو في أساس تحقيق هذا النظام للنجاح الملحوظ.

(٩) شركة ماستر كارد طورت نظاماً أسمته Secure Electronics Payment Protocol – SEPP في حين كان اسم مشروع شركة فيزا Secure Transaction Technology

(١٠) ومن بين الشركات التي انضمت لاحقاً: GTE, IBM, Microsoft, Netscape, Teresa Systems,. Verisign، راجع حول هذا الموضوع:

Sédaillan V., Droit de L'Internet. Collection AUI 1997. p.221.

والعمليات المالية وغير المالية الحاصلة في الشبكة عن طريق تأمين خدمة نقل البيانات ذات الطابع السري والمهم بشكل مشفر(١١).

المطلب الثاني: صور الاستخدام غير المشروع لبطاقة الدفع الإلكتروني عبر شبكة الإنترنت:

الفرع الأول : الحصول على أرقام بطاقة الدفع الإلكتروني عبر شبكة الإنترنت:

تمكن بعض الهواة والمحترفين من معتادي التعامل مع شبكة الإنترنت الذي يطلق عليهم تسمية (Hackers)(١٢)، من التقاط أرقام بطاقة الدفع الإلكتروني الخاصة ببعض العملاء من الشبكة واستخدموا أرقامها في الحصول على السلع التي يرغبونها وخصم القيمة من حساب العملاء الشرعيين لهذه البطاقة(١٣).

وهناك عدة طرق يتبعها قراصنة الحاسب الآلي والإنترنت في الحصول على بيانات بطاقات الوفاء واستعمالها بطرق غير مشروعة للحصول على السلع

---

(١١) انظر:
Nguyen (H.), Des Paquts Cryptés Pour Sécuriser Le Paiement Sur Le Web, Le Monde Interactif (Le Monde Esition Proche – Oriect), 23 juin 2000, p.4.

(١٢) استعمل هذا المصطلح لاول مرة في الستينات بواسطة مجموعة من الطلبة الذين يدرسون في الجامعات الأمريكية ويتمّتعون بقدر عال من الكفاءة، ويتفاخرون بإلمامهم بعلوم الكمبيوتر، وبإمكانية اختراقهم لشبكات الحاسبات الآلية بجهودهم الذاتية وبدون تعليمات.
ويعني حالياً مصطلح (Hackers) الشاب البالغ الذي ينتهك بدون إذن الشبكات المعلوماتية عن طريق كمبيوتره، حيث يمكنه الدخول إلى الكمبيوترات الأخرى، وعلى نحو غير مشروع، باستعمال (Modem) وهو جهاز له قدرة على تحويل النبضات الرقمية إلى موجات إلكترونية التي يمكن نقلها بدورها على خط تلفوني.

(١٣) جميل عبد الباقي الصغير، المرجع السابق، ص٣٦.

والخدمات أو لغايات استعمال هذه البيانات في عمليات تزوير البطاقة وهذه الطرق هي:

١- الاختراق غير المشروع لمنظومة خطوط الاتصالات العالمية(Illegal Access).

وهي الخطوط التي تربط الحاسب الآلي للمشتري بذلك الخاص بالتاجر، ويعد الجاني هنا بمثابة من يتصنت على مكالمة هاتفية، وهذا الأسلوب من اخطر ما يهدد التجارة عبر الشبكة؛ ذلك أنّ الدافع الأساسي وراء اللجوء إليه، يتمّثل في رغبة كامنة في نفوس محترفي إجرام التقنية ــ وقراصنة البطاقات أحد طوائفهم ــ في قهر نظم التقنية، والتفوق على الحماية المقررة لها وتعقيداتها(١٤).

وإمعاناً في التحدي تقوم معظم العصابات التي تضم قراصنة البطاقات بنشر هذه المعادلات، وبيان الكيفية التي يمكن من خلالها إتباعها خطوة بخطوة بهدف الحصول على الأرقام الخاصة ببطاقات الوفاء المملوكة للغير، وذلك عبر مواقعهم على شبكة الإنترنت(١٥).

ورغم صعوبة تحديد شخصية محترفي أنظمة المعلومات، إلا أنه يمكن تحديد كيفية الاختراق وزمانه، وكلمة السر التي استخدمت في الاختراق، وذلك من

---

(١٤) عماد علي خليل: التكييف القانوني لإساءة استخدام البطاقات عبر شبكة الإنترنت. مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات العربية، العين، دولة الإمارات العربية المتحدة، ٢٠٠٠. ص٣.

(١٥) من مواقعهم على الشبكة تحت بند (How To Hack A card)

١. www. Dark –secrets. Com

٢. www. Hackers/resets/credit/credit 3 txt

خلال مراجعة ملفات الدخول للنظام والملفات التأمينية الخاصة به، على نحو يسمح بجمع أكبر قدر من الأدلة التي تشير للجاني(١٦).

في عام ٢٠٠٤ أعلن مكتب التحقيقات الفيدرالي (FBI) أنه يحقق في حادث اختراق أجهزة كمبيوتر تمّ خلاله سرقة أرقام ثمانية ملايين بطاقة وفاء من شركة "Data processors International" التي تجري عملية تحول مالية لشركات فيزا، وماستركارد وأمريكان اكسبرس التي تعرضت لاختراق في نظام العمل من طرق خارجي غير مصرح له بالدخول على النظام.

كما أعلنت شركتا فيزا وماستركارد أنّ أحد قراصنة الكمبيوتر استطاعوا اختراق (٢,٢) مليون حساب تابع للشركتين، واستطاع القرصان أن يتجاوز أنظمة تأمين شركة تقوم بإنجاز التعاملات الخاصة للبطاقتين نيابة عن التجار(١).

٢- تقنية تفجير الموقع المستهدف (Corruption of Requested Site).

ويستند هذا الأسلوب إلى ضخ مئات الآلاف من الرسائل الإلكترونية (E-mails) من جهاز الحاسب الآلي بالقرصان إلى الجهاز المستهدف بهدف التأثير على ما يعرف (بالسعة التخزينية)، بحيث يشكل هذا الكم الهائل من الرسائل الإلكترونية ضغطاً يؤدي في المحصلة إلى تفجير الموقع العامل على الشبكة، وتشتت المعلومات والبيانات المخزنة فيه، لتنتقل بعد ذلك إلى الجهاز الخاص بالقرصان، ليتمّكن الأخير من حرية التجول في الموقع المستهدف بسهولة،

---

(١٦) جميل عبد الباقي الصغير، المرجع السابق، ص٣٨.

(١٧) انظر: www.gn4me.com/etesalat/article.jsp?artid=7789.

ويسر والحصول على كل ما يحتاجه من أرقام وبيانات ومعلومات خاصة ببطاقات وفاء مملوكة لغيره(١٨)

وهذه الطريقة توجه إلى الحواسيب المركزية للبنوك، والمؤسسات المالية والمطاعم والفنادق ووكالات السفر، بهدف تحصيل اكبر عدد ممكن من أرقام البطاقات(١٩).

٣- أسلوب الخداع: (Fallx Commerant)

ويتحقق بإنشاء مواقع وهمية على شبكة الإنترنت على غرار مواقع الشركات والمؤسسات التجارية الأصلية الموجودة على الشبكة، ويظهر هذا الموقع وكأنه الموقع الأصلي الذي يقدم الخدمة، ولكي ينشأ هذا الموقع يقوم القراصنة بالحصول على بيانات الموقع الأصلي كافة من خلال شبكة الإنترنت، ومن ثمّ إنشاء الموقع الوهمي، ومع تعديل البيانات السابقة التي تمّ الحصول عليها بطريق غير مشروع – وذلك في الموقع الأصلي – حتى لا يظهر أن هناك ازدواجاً في المواقع، ويبدو الموقع الأصلي، وكأنه الموقع الوحيد(٢٠).

ويتحقق الضرر باستقبال الموقع الوهمي ــ الخاص بالقراصنة ــ على شبكة الإنترنت لكافة المعاملات المالية والتجارية الخاصة بالتجارة الإلكترونية التي يقدمها الموقع الأصلي عبر الشبكة لأغراض هذه التجارة، ومنها بالطبع بيانات بطاقة الدفع الإلكتروني، وكذلك الرسائل الإلكترونية الخاصة بالموقع الأصلي،

---

(١٨) عبد الفتاح بيومي حجازي، الكتاب الأول، المرجع السابق، ص١٣٢.

(١٩) عماد علي خليل، التكييف القانوني لإساءة استخدام البطاقات عبر شبكة الإنترنت، المرجع السابق، ص٣٤.

(٢٠) جميل عبد الباقي الصغير، المرجع السابق، ص٣٧.

ومن ثمّ يتسنى الإطلاع عليها والاستفادة غير المشروعة من المعلومات المتضمنة فيها، على نحو يضر بالمؤسسات والشركات صاحبة الموقع الأصلي، وفي الوقت نفسه يدمر ثقة الأفراد والشركات في التجارة عبر الشبكة(٢١).

ولذلك تأتي أهمية اتخاذ إجراءات أمنية ــ معلوماتية ــ لمنع إساءة استخدام بطاقات الدفع الإلكترونية، وهذا ما بدأت به المؤسسات المالية المُصدرة لهذه البطاقات، من إصدار بطاقات ذات سقف مالي محدود بحيث إذا سرب رقمها أو فقدت كان الضرر يسيراً للعميل والمؤسسة المالية، لكن هذا الضمان غير مجدٍ في عمليات التجارة الإلكترونية التي تقدر عملياتها بمئات الملايين من الدولارات التي تنساب عبر الشبكة يومياً(٢٢).

ولهذا نرى أن الإنتاج في ميدان التقنية العالية، يتجه منذ عشرات السنين إلى زيادة إنتاج وسائل الحماية التقنية أكثر من إنتاج التقنية نفسها، فمجرمو التقنية تفوقوا على أنفسهم عندما ارتكبوا الاعتداء على أنظمة الحماية ذاتها والتي صممت لمنع الاعتداء على أنظمة التقنية العالمية، بما تشتمل عليه هذه الأنظمة من حواسيب، وبرامج وشبكات ربط واتصال(٢٣).

---

(٢١) علي حسني عباس، مخاطر بطاقات الدفع الإليكتروني عبر شبكة الإنترنت، المشاكل والحلول، ورقة عمل مقدمة في ندوة الصورة المستحدثة لجرائم بطاقات الدفع الإليكتروني، نظمت بمعرفة مركز بحوث الشرطة، أكاديمية الشرطة، القاهرة، جمهورية مصر العربية ١٩٩٨/١٢/١٤، ص١٧.

(٢٢) عبد الفتاح بيومي حجازي، الكتاب الأول، المرجع السابق، ص١٣٣.

(٢٣) راجع في ذلك الواقعة المتعلقة باختراق نظام معلوماتي في أحد المصارف الشهيرة انفق عليه الكثير بمعرفة المؤسسات المالية وعن طريق خبراء المعلوماتية الذين قضوا شهوراً في إعداد النظام، وتمَّ اختراقه يوم افتتاحه أمام الصحفيين من قبل الهاكرز إمعاناً في تحديهم لهذه الأنظمة

ومن صور الخداع، قيام القراصنة بصفتهم الجهات المُصدرة لبطاقات الوفاء بإرسال رسائل إلكترونية يطلبون فيها من المستقبلين تجديد المعلومات الخاصة بهم، مثل الاسم، والعنوان، ومعلومات البطاقة، وإرسالها مرة أخرى إلى الموقع وبذلك يحصلون على أرقام البطاقات(٢).

٤-تخليق أرقام البطاقة (Card Math):

وهو يعني تخليق أرقام بطاقة وفاء اعتماداً على إجراء معادلات رياضية وإحصائية، وهي كل ما يلزم للشراء عبر شبكة الإنترنت، فهذا الأسلوب يعتمد على أسس رياضية في تبديل وتوفيق لأرقام حسابية تؤدي في النهاية لناتج معين هو (الرقم السري) لبطاقة وفاء متداولة، ويتمّ استخدامها في معاملات غير مشروعة، عبر الشبكة، ومن هنا تأتي خطورة أن يكون كود البطاقة أو رقمها السري هو الضمان الوحيد لعدم اختراقها أو إساءة استعمالها(٣).

(عماد خليل: التكييف القانوني لإساءة استخدام البطاقات عبر شبكة الإنترنت، المرجع السابق. ص٤).

(٢) أرسلت شركة Register المتخصصة في تسجيل أسماء البطاقات رسالة إلى زبائنها تحذرهم فيها من الاستجابة إلى رسائل يقوم أحد المواقع بإرسالها إلى زبائنها تطلب منهم تجديد المعلومات الخاصة بهم وإرسالها مرة أخرى إلى الموقع، وأضافت الشركة أن الرسائل تصل من موقع www.Renewal-center.com.

كما اشتكى عدد من مستخدمي الموقع www.ebay.com إلى الـ (FBI) من وصول رسائل البريد الإلكتروني خادعة تبدو أنها مرسلة من الموقع المذكور، تطلب منهم تحديث معلوماتهم الشخصية مثل أرقام بطاقاتهم الائتمانية، وأسماء أمهاتهم قبل الزواج، وورد في الرسائل تهديد بوقف حساباتهم في الموقع إذا لم يقوموا بذلك.

(٣) عماد علي خليل، التكييف القانوني لإساءة استخدام البطاقات عبر شبكة الإنترنت، المرجع السابق، ص٥.

ولخطورة الأبعاد المترتبة على هذا النشاط غير المشروع يرى أحد المحققين في الشرطة الفيدرالية الأمريكية (FBI)، وأحد المتخصصين في الإنترنت في مؤلفه (Card Fraud) بقوله: (كيف صارت بطاقة الائتمان مطمع الأجيال الجديدة، من قراصنة الجريمة المنظمة، وكيف صارت أرصدة الدول والأفراد نهباً مشاعاً لمجرم متعلم يستند إلى مبادئ بسيطة في علم الإلكترونيات، والحاسب وطرق التشغيل، والبرمجة والتعامل مع الإنترنت؟ وكيف تكون في (هونج كونج) أو في (نيجيريا) وتسرق شخصاً آمناً في أوروبا أو كندا أو أمريكيا أو البلاد العربية؟ تسرق دون أن تلتقي بالضحية، ودون أن تدخل بيته، أو تفتح خزانته، ودون أن تحمل سلاحاً أو تريق قطرة دم، إنها جريمة السرقة عن بعد، وفي عالم الريموت كنترول تأتي السرقة بالريموت، ولكن دون كنترول)[٢٤].

٥- أسلوب التجسس (Spying):

حيث يقوم قراصنة الكمبيوتر باستخدام البرامج التي تتيح لهم الإطلاع على البيانات والمعلومات الخاصة بالشركات، والمؤسسات التجارية العاملة على شبكة الإنترنت، وبالتالي يتمّكنون من الحصول على ما يريدون من المعلومات، ومنها المتعلقة ببطاقات الوفاء التي استخدمت في التجارة الإلكترونية عبر الشبكة[٢٥].

ومن الأمثلة على هذا الأسلوب ما قام به طالبان جامعيان في مدينة بور سعيد المصرية، من سحب مبلغ نصّف مليون جنيه من رصيد أحد عملاء البنوك

---

(٢٤) Neuton: Card Fraud. P: 200.

(٢٥) علي حسني عباس، المرجع السابق، ص٢٥.

الحكومية عن طريق شبكة الإنترنت، واستخدما هذه المبالغ في مشاهدة أفلام متنوعة على الإنترنت، وتبين أنهما استطاعا معرفة الرقم السري لحساب العميل على هذه الشبكة عن طريق التجسس واستغلاه في مشاهدة هذه الأفلام على مدى سبعة شهور(٢٦).

٦- تبادل المعلومات (Exchange of Information).

يقوم قراصنة الكمبيوتر بتبادل المعلومات التي يحصلون عليها عن أرقام البطاقات، وعن أفضل الطرق للدخول غير المشروع، وكيفية الحصول على المعلومات فيما بينهم من أجل التوسع في استخدام الأرقام، وأن يكون هذا الاستخدام صادراً من بلدان مختلفة.

ففي قضية حدثت في الأردن تتلخص وقائعها أن شخصاً يدعى (س.ع.ع.ش)، يحوز على أرقام بطاقات وفاء دولية مسروقة، ويقوم باستخدامها عبر شبكة الإنترنت لشراء برامج/وأفلام خلاعة يستقبلها عبر صندوق بريده، وبتفتيش منزله تمّ ضبط جهاز كمبيوتر، ولوحات إلكترونية وأشرطة (CD) و(Floppy) وبالتحقيق معه أفاد بأنه حصل على أرقام البطاقات المسروقة من شخص في بريطانيا (٩٧).

---

(٢٦) مشار لهذه الواقعة في جميل عبد الباقي الصغير، المرجع السابق، ص٣٨.

(٩٧) كتاب إدارة مكافحة المخدرات/قسم تزييف البطاقات، رقم ٢/٢٠٠٠/بطاقات/٧٣٨٩ تاريخ ٢٠٠٠/٧/٦.

الفرع الثاني : القيام باستخدام البطاقة في عمليات غسل الأموال.

وفي هذه الحالة، فإنّ البطاقة المستخدمة في عملية الوفاء أو التحويل، هي بطاقة صحيحة ومستخدمة من قبل حاملها الشرعي، إلا أن الغاية التي استخدمت من أجلها غير مشروعة، ولا تعد من الوظائف التي استحدثت البطاقة لأجلها.

فقد أثار استخدام بطاقة الدفع الإلكتروني كبديل للتعامل بالنقود الورقية العديد من المشكلات وخاصة ما تعلق منها بغسيل الأموال، ذلك أنّ التعامل المالي باستخدام هذه البطاقات لا يكون من المستطاع تعقبه، أو الوقوف على أثره، وهو ما يجعل المبدأ السائد في التعامل البنكي "اعرف عميلك" مبدأ يصعب تطبيقه، والأخذ به، فضلاً على أن التعامل بهذه البطاقات يتمّ مباشرة بين شخصين ولا يقتضي تدخلاً من المؤسسة المالية، كما أنّ هذه التعاملات تتم بسهولة وبسرعة، إذ تكفل تحويلاً فورياً للمال من والى أي مكان في العالم، ويكون المتعامل فيها مجهول الشخصية، ودون حواجز أو قيود قانونية(٢٧).

وتتم عملية غسيل الأموال بواسطة بطاقة الدفع الإلكتروني بطريقتين(٢٨):

---

(٢٧) أشرف توفيق شمس الدين، مدى ملائمة تجريم غسيل الأموال للقواعد المصرفية، ورقة عمل مقدمة إلى مؤتمَّر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، نظمته جامعة الإمارات العربية المتحدة، ٩ – ١١/ربيع الأول/ ١٤٢٤هـ الموافق ١٠ – ٢٠٠٣/٥/١٢، المجلد الرابع، ص١٤٢٧.

(٢٨) تؤكد الإحصائيات والتقارير الاقتصادية أن ظاهرة غسيل الأموال تتصاعد بشكل مخيف في ظل العولمة الاقتصادية وشيوع التجارة الإلكترونية، حيث يتمّ الغسيل الإلكتروني في دقائق، أو ثواني معدودة من أجل الإسراع في إخفاء هذه العمليات وقدر خبراء الاقتصاد المبالغ التي يتمّ غسلها سنوياً بـ(ترليون دولار)، وهو ما يعادل (١٥%) من إجمالي قيمة التجارة العالمية.

أ- استخدام البطاقة في أجهزة الصرّاف الآلي:

وغالباً ما يقوم العميل باستصدار طلبات متتالية للبنك المُصدر لإصدار بطاقات وفاء للاستخدام محلياً ودولياً له ولموظفيه ومعاونيه وأفراد عائلته، ولأي أفراد آخرين يتعاملون معه بضمان ودائع الشركة النقدية أو العينية ويتمّ استخدام هذه البطاقات في مجال التحويلات المالية الإلكترونية عن طريق أجهزة الصرّاف الآلي في عمليات غسيل الأموال، بحيث يتمّ إجراء التحويلات المالية إلكترونياً التي تصل من الخارج، وقبل أن تستقر يتمّ سحبها إلكترونياً أيضاً ثم يتمّ تجميعها، ويقوم العميل بتحويلها بمبالغ كبيرة إلى الخارج.

ويقوم العميل بصرف المبالغ عن طريق البطاقة من أجهزة الصرّاف الآلي باستخدام رقمه السري ثم يقوم الفرع الذي صرف منه، أو من خلال أجهزته بطلب تحويل المال إليه من الفرع مصدر البطاقة، فيقوم الأخير على هذا الأساس بالتحويل تلقائياً وخصم القيمة من حساب عميله والذي يكون قد تهرب بهذه الطريقة من القيود التي تكون مفروضة على التحويلات(٢٩).

انظر: زغلول محمود البلشي: مسئولية البنك الجنائية عن جرائم غسيل الأموال، ورقة عمل مقدمة إلى مؤتمَّر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المشار إليه سابقاً، المجلد الخامس، ص١٩١٥.

(٢٩) نصّت المادة الخامسة من تعليمات مكافحة عمليات غسيل الأموال رقم (٢٠٠١/١٠) الصادرة عن البنك المركزي الأردني بقولها: "يجب على البنك التأكد من هوية أي شخص ليس لديه حسابات في البنك، ويرغب بالدفع نقداً مقابل حوالات في جميع الحالات التي يكون مبلغ المعاملة (١٠) آلاف دينار أو أكثر أو ما يعادلها بالعملات الأخرى".

وفي ذلك نصّت المادة (٥) من التعميم رقم (٢٠٠٠/٢٤) الصادر عن مصرف الإمارات العربية المتحدة المركزي في ٢٠٠٠/١١/١٤ بقولها: "١. بالنسبة لمن ليست لهم حسابات في البنوك ويرغبون بالدفع نقداً مقابل الحوالات يجب على البنوك، والصرافات التحقق بعناية وانتظام من

وحيث إنّ بطاقات الصرّاف الآلي (ATM) تمكن حامليها من سحب الأموال محلياً ودولياً ــ عبر (٥٣) دولة في العالم[٣٠] ــ فهذا سهّل مهمة غاسلي الأموال بتهريب الأموال المشبوهة، وقد اكتشفت السلطات الأمريكية من خلال التقارير أنّ الأموال المودعة في بعض البنوك والمصارف الأمريكية يتمّ سحبها بواسطة أجهزة الصرّاف الآلي في بعض الدول المنتجة للمخدرات، وأن هذه العمليات تتم بصورة متكررة[٣١].

ب- غسيل الأموال بواسطة الوفاء بالبطاقة.

وتتم هذه العملية على ثلاث مراحل:

المرحلة الأولى: الإيداع أو الإحلال.

حيث يتمّ إيداع الأموال المشبوهة في أحد البنوك سواء المحلية، أم الخارجية، والحصول على بطاقات وفاء بسقف يعادل الرصيد المودع.

المرحلة الثانية: الخداع والتمويه.

هوية أي عميل من هؤلاء التي فيها تكون قيمة المعاملة المصرفية (٢٠٠) ألف درهم أو أكثر أو ما يعادلها بالعملات الأخرى، وفي هذا السياق يشمل التحقق عادة تفاصيل العميل وإدخالها في النموذج رقم (م م ٩/٢٠٠٠/١).

٢. في حالة استلام تحويل لكي يدفع نقداً أو على شكل شيكات مسافرين لأشخاص ليس لديهم حسابات في البنك أو وردت عن طريق إحدى الصرافات وكان مبلغها (٢٠٠) ألف درهم أو أكثر أو ما يعادلها بالعملات الأخرى، فيجب ملء النموذج رقم (م م٩/٢٠٠٠/٢)".

(٣٠) أروى فايز الفاعوري وإيناس محمد قطيشات، جريمة غسيل الأموال (المدلول العام والطبيعة القانونية)، دار وائل للنشر، عمّان، الأردن، الطبعة الأولى، ٢٠٠٢، ص٩٥.

(٣١) حسام العبد، غسيل الأموال الإلكتروني، مجلة البنوك في الأردن، العدد السابع، أيلول،٢٠٠٠، المجلد ١٩، ص٧٨٩٩.

حيث تستخدم هذه البطاقات فيما بعد في شراء الأصول المادية كالمعادن الثمينة واللوحات الفنية باهظة الثمن، وتكون عملية الشراء مباشرةً، أو عن طريق الغير بتسليمه بطاقة الدفع الإلكتروني، أو بواسطة الإنترنت مع اللجوء إلى استخدام أنظمة الحماية والتشفير لضمان سرية العمليات التي تتم عبره.

المرحلة الثالثة: الدمج والإعلان.

حيث يجري بيع الأصول المادية نقداً، أو لقاء شيك، أو حوالة مالية مسحوبة على بنك آخر(٣٢).

وقد أصبحت بطاقة الدفع الإلكتروني تستخدم بشكل واسع مؤخراً في عمليات غسيل الأموال نظراً للتطور السريع الذي يحدث لتسهيل الدفع والتحويلات، مثل استخدام الهاتف والإنترنت إلكترونياً في الإجراءات البنكية، مما مكن غاسلي الأموال من استخدام بطاقة الدفع الإلكتروني في تحويل كميات كبيرة من المال بلا مخاوف من كشف هويتهم، وخاصة لما تتميز به هذه البطاقة من سهولة حملها عبر حدود البلاد، واستخدامها على المستوى الدولي، وصعوبة كشف مصدر المال عن طريقها.

ومن أشهر هذه البطاقات (الكارت الممغنط الذكي) لما له من خاصية الاحتفاظ بملايين الدولارات مخزنة على القرص الخاص به، وإمكان نقل هذه الأموال إلكترونياً على كارت آخر بواسطة الهاتف المعد لذلك ودون تدخل أي بنك من

---

(٣٢) م حسن الخضيري، غسيل الأموال "الظاهرة وأسباب العلاج"، مجموعة النيل العربية، القاهرة، جمهورية مصر العربية، ٢٠٠٣، ص١١٩-١٢٢.

البنوك، أي بمنأى عن أي رقابة أو إشراف مما يمهد الطريق لغسيل الأموال بأسلوب دقيق، وعملية محكمة يصعب اكتشافها أو تعقبها(٣٣).

ونظراً للطبيعة الدولية لعمليات غسيل الأموال، فقد قامت بعض المنظمات الدولية المتخصصة في هذا المجال برصد الطرق المستحدثة لغسيل الأموال عبر الإنترنت، حيث يوفر الاستخدام المتنوع لتلك الشبكة والمتطور العديد من الأنشطة المصرفية الإلكترونية كالبنوك الافتراضية أو بنوك الإنترنت(٣٤) التي هي في الواقع ليست بنوكاً من النوع المألوف إنما عبارة عن وسيط في القيام ببعض العمليات المالية وعمليات البيوع، وهذه الوسيلة تتيح لغاسلي الأموال تحويل أو نقل كميات هائلة من الأموال بسرعة وأمان، إذ إن المتعاملين فيها غير معلومي الهوية كما أنّها لا تخضع قوانين، أو تعليمات رقابية وتتم عبر الحدود الدولية دون رقابة أو إمكانية تعقبها، وهذه التحويلات عبر الإنترنت يمكن إتمامها باستخدام بطاقة الدفع الإلكتروني، إذ يتمّكن غاسلو الأموال بهذه الطريقة من تحويل أرصدتهم عدة مرات يومياً في أكثر من بنك حول العالم(٣٥).

---

(٣٣) جلال محمدين، دور البنوك في مكافحة غسيل الأموال، دار الجامعة الجديدة للنشر، الإسكندرية، جمهورية مصر العربية، ٢٠٠٠، ص٣٧.

(٣٤) موقع مجموعة العمل المالية FATF على العنوان : www.ustreas.gov/finance/fatfre98.

(٣٥) انظر:

Scott Seltzer, Money Laundering: The Scope of the Problem and Attempts to Combat والمشار إليه في جلال محمدين، المرجع السابق، ص ٣٥.

ومن أشهر الأمثلة على عمليات غسيل الأموال باستخدام بطاقة الدفع الإلكتروني(٣٦):

١- ما حدث في الولايات المتحدة الأمريكية حيث استطاع غاسلو الأموال من تركيب أجهزة صرّاف آلية مصنّعة وتكوينها استطاعوا عن طريقها من اكتشاف ومعرفة الأرقام السرية للعملاء المستخدمين لها، ثم قاموا بتزوير البطاقات واستخدامها في عمليات السحب والإيداع عن طريق ماكينات حقيقة بالفعل، وبالتالي تمّ غسيل العديد من الأموال بهذه الطريقة حتى تمّ اكتشافها.

٢- تمّ اكتشاف أحد تجار المخدرات يقوم بعملية غسيل لأمواله عن طريق فتح حسابات لبطاقات وفاء بعدة بنوك، وإيداع مبالغ مالية على دفعات بها حتى تبدو التحويلات فيما بعد طبيعية، ثم يقوم بالسفر إلى بلد آخر يتواجد به أحد شركاؤه الذي يمتلك محل للمجوهرات يستغله كواجهة للتضليل والخداع فيدفع له باستخدام بطاقات الوفاء في عمليات شراء مجوهرات بأثمان باهظة، وهي مجرد عمليات وهمية حتى يستطيع شريكه تحصيل هذه المبالغ من البنوك مصدرة البطاقات ليتمّ بعد ذلك استخدامها في شراء مواد مخدرة أو دفعها مقابل مخدرات تمّ تسليمها بالفعل.

٣- وفي بريطانيا تمكنت الشرطة البريطانية في شهر تموز من عام ١٩٩٥ من ضبط أكبر عصابة متخصصة في تزوير بطاقات الوفاء في تاريخ

---

(٣٦) سامح محمد عبد الحكم، الحماية الجنائية لبطاقات الائتمان "جرائم بطاقات الدفع الإلكتروني"، دار النهضة العربية، القاهرة، جمهورية مصر العربية، ٢٠٠٣،ص ١٠٣- ١٠٤.

بريطانيا، وعثرت الشرطة على (٨٠) ألف بطاقة مزورة وتمكنوا من اعتقال أفراد العصابة التي تبين من خلال التحقيقات أنها كانت تنوي سحب مائة مليون جنية إسترليني بواسطة هذه البطاقة من حساب عملاء حقيقيين للبنوك البريطانية وتحويل هذه الأموال إلى بنوك أخرى خارج بريطانيا ليتسنى إضفاء صفة المشروعية عليها وعودة هذه الأموال للبلاد مرة أخرى بصورة مختلفة، ومشروعة.

٤- تقوم بعض المنظمات غير الشرعية باستخدام بطاقة الدفع الإلكتروني في التجارة غير المشروعة عبر شبكة الإنترنت، وغسلهم لأموال مستحصلة من تجارة المخدرات، والأعضاء البشرية، والدعارة الدولية، وبيع الأطفال وذلك بإيداعهم لأموال مسحوبة بطرق غير شرعية بحسابات عائدة بالبنوك ثم يقومون بتحويلها بين عدة فروع حتى تنقطع الصلة بين المُصدر غير المشروع لها، واستخدامها بعد ذلك في سداد المدفوعات، وإمكانية السحب منها بعد ذلك باستخدام البطاقة.

المبحث الثاني

الوسائل الوقائية للحد من الاستخدام

غير المشروع لبطاقة الدفع الالكتروني عبر الانترنت

أمام تزايد عمليات الاستخدام غير المشروعة لبطاقة الدفع الإلكتروني التي تقدّر وفقاً لآخر التقديرات الصادرة عن لجنة التجارة الفيدرالية الأمريكية لعام (٢٠٠٢) بنحو (٤٨) مليار دولار أمريكي سنوياً، كما تكلّف المستهلك نحو

خمسة مليارات دولار سنوياً [٣٣]، فقد قامت الجهات المُصدرة لبطاقة الدفع الإلكتروني بوسائل وقائية تتمثل بإجراءات تكنولوجية وأخرى إدارية للحد من هذه الاستخدامات غير المشروعة لبطاقة الدفع الإلكتروني.

كما أنّ هذه الإجراءات لا تقتصر فقط على الجهة المُصدرة، وإنما هناك إجراءات أخرى يجب أن يقوم بها التاجر تتمثل باكتشاف الاستخدام غير المشروع عند وقوعه، وكذلك يقوم بها الحامل تتمثل بالوقاية من وقوع البطاقة في عمليات الاستخدام غير المشروع.

وسوف أتناول الإجراءات المتخذة من قبل المُصدر في مطلبٍ أول، والإجراءات المتخذة من قبل الحامل والتاجر في مطلبٍ ثانٍ.

المطلب الأول:الإجراءات المتخذة من قبل المُصدر

تتمثل الإجراءات التي يقوم بها المُصدر من أجل حماية البطاقة من الاستخدامات غير المشروعة المصاحبة لها، إما بتطوير البطاقة تقنياً من أجل الحد من عمليات تزويرها، أو القيام بعدد من الإجراءات الأخرى تساهم في مواجهة الاستخدامات غير المشروعة، وسوف أتناول هذه الإجراءات في الفرعين التاليين:

الفرع الأول: الإجراءات التقنية.

من أجل الحد من عمليات التلاعب وتزوير البطاقة، تقوم الجهات المُصدرة وبالتعاون مع شركات التقنية التكنولوجية بتطوير بطاقة الدفع الإلكتروني بشكل دائم، آخذين بعين الاعتبار مواجهة طرق التزوير التي تمت في السابق.

---

(٣٧) انظر: شبكة النبأ المعلوماتية – الاثنين ٢٠٠٣/١٢/١٥.

وأول حلقات هذا التطوير كان باختراع بطاقة ذات دوائر إلكترونية[٣٤]، والمزايا التي تتمتع بها هذه البطاقة أنها غير قابلة للتأثير عليها أو اختراقها كما أنّها تحتفظ في ذاكرتها بآخر العمليات المنفذة، وهذا يؤدي إلى نتائج قانونية متعلقة بالإثبات، كما أنّها تُعدّ من الناحية التقنية غير قابلة للتزوير سواء من ناحية المادة المصنوع منها البطاقة وهي مادة (PVC) أو (PVCA)، أم من ناحية إدخال (Heliogram) وهي استخدام حزم الليزر التي تعكس صورة الشيء المراد تصويره على مكان التصوير، ومثاله صورة الحمامة في بطاقة الفيزا[٣٥].

وثاني حلقات التطوير، كان بإدخال البطاقة الذكية (Smart Card) إلى بيئة البطاقات، وهي عبارة عن بطاقة بلاستيكية من حجم بطاقة الدفع الإلكتروني، وتضم شرائح ذات دوائر متكاملة قادرة على تخزين البيانات ومعالجتها[٣٦].

ومن بين الإجراءات التقنية لمواجهة إساءة استخدام بطاقات الوفاء من خلال الإنترنت النموذج التقني الموحّد الذي أعلنت عنه شركتي فيزا (Visa) وماستر كارد (Master Card) بتاريخ ١٩٩٦/٢/١، والمسّمى نظام الصفقات الإلكترونية الآمنة (SET) (Secure Electronics Transactions Protocol) وبعد ذلك أنّضم لهذا المشروع شركات أمريكية أخرى[٣٧].

---

(٣٨) يرجع الفضل في اختراع هذه البطاقة إلى المهندس الفرنسي رونالد مورينو في عام ١٩٧٤.

(٣٩) للمزيد من التفصيل في وصف البطاقة ومزاياها انظر: كيلاني عبد الراضي محمود: المسئولية عن الاستعمال غير المشروع لبطاقات الوفاء والضمان، دار النهضة العربية، القاهرة، جمهورية مصر العربية، ٢٠٠١، ص٢٣٠.

(٤٠) للمزيد من التفصيل حول البطاقة الذكية انظر:
John Wright: "Smart Card: Legal and Regulatory Challenges" The Bankers Magazine, (March –April, 1997) , pp. 24 – 28.

(٣٧) من بين الشركات التي انضمت لاحقاً: GTE ,IBM , Microsoft, Netscape , SAIC , Teresa systems

وأعلنت ماستر كارد العالمية في عام (٢٠٠٢) عن طرح بطاقة (ماستر كارد باي باس)، وهو برنامج للدفع بالبطاقة دون اتصال يوفر للعملاء طريقة مبسطة للدفع، وتُعدّ بطاقة دفع مطورة تمتاز برقاقة كمبيوتر مضمنة ومخفية وأنتينا (لاقط) وكل ما على حامل البطاقة فعله هو تمرير البطاقة أمام، أو قرب جهاز إلكتروني مهيأ خصيصاً لدى التاجر، وبعدها تقوم البطاقة بإرسال معلومات الدفع لاسلكياً ملغية الحاجة إلى أن يقوم حامل البطاقة بتسليم بطاقته إلى التاجر الذي يمررها خلال جهاز قارئ، ويتمّ بعد ذلك تبادل معلومات الحساب مباشرة مع الجهاز الإلكتروني، ثُمّ معالجتها من خلال شبكة ماستر كارد الموثوقة لقبول أوامر الدفع، وبعد لحظات من تمرير حامل البطاقة بطاقته (ماستر كارد باي باس) أمام الجهاز الإلكتروني يستلم إشارة بتأكيد الدفع بينما يكون هو في طريقه إلى منزله أو عمله(٣٨).

وتتأهب حالياً شركة أمريكية، وهي شركة (ابلايد ديجيتال سوليوشينز) (IDS) عُرفت بتطوير رقائق تزرع تحت الجلد لتحديد الهوية الشخصية التعرف على موقع حامليها، لتأمين طريقة موثوقة لزبائنها لتفادي الغش، بتوظيف الرقائق في تعاملات الدفع ببطاقة الدفع الإلكتروني، وأسمتها (رقيقة فيريتشيب)، وقُدّمت الرقيقة كطريقة متفوقة على بطاقة الدفع الإلكتروني الحالية، والبطاقة الذكية اللتين باتتا – وفي غياب تقنيات معتمدة للقياسات البيولوجية وتقنيات سلامة مناسبة – معرضتين للسرقة وللتزوير.

(٣٨) مجلة اتحاد المصارف العربية، العدد (٢٢٦)، كانون الثاني/ ٢٠٠٣، ص٦٩-٧١.

وقالت الشركة أثناء المؤتمر العالمي للهوية لعام (٢٠٠٣) الذي عقد في باريس: "إن الرقيقة (فيريتشيب) يجب تسميتها (الحل الواقي من الضياع)، وإن طريقتها الفريدة بإنغراسها تحت الجلد يمكن استخدامها لحالات متنوعة من تأكيد الهوية على الصعيدين المالي، والأمني على حد سواء.

وتطرح حالياً وللمستقبل تطبيقات لتقنيات جديدة مثل تقنية تحديد الترددات الراديوية في التعرف على الهوية (RFID)، والقياسات البيولوجية، والبطاقات الذكية، وجمع المعلومات، إلا أن أنواع الرقائق (فيريتشيب) وهي من نوع (RFID) تحمل رقم هوية خاصاً بكل واحد منهما، وتستطيع أن تحمل أيضاً معلومات خاصة أخرى عن حاملها المزروعة فيه، وعندما تمر طاقة الترددات الراديوية من الكاشف إلى الرقيقة فإنّ الرقيقة تتحرك، إذ إنها لا تغذى بطاقة مستقلة، وتبدأ ببث إشارات راديوية عن المعلومات الموجودة داخلها، يلتقطها الجهاز القارئ الموصول بكمبيوتر المُصدر(٣٩).

ومن الشركات العربية التي ساهمت في إطلاق بطاقة وفاء آمنة للتسوق عبر الإنترنت شركة "مكتوب دوت كوم" حيث أعلنت عن إصدار بطاقة "كاش يو" التي تمكن الحامل من شراء السلع والخدمات على شبكة الإنترنت بثقة تامة دون أية مخاطر ممكنة وهي متوافرة بثلاث فئات: عشرة دولارات، عشرين دولاراً، ثلاثين دولاراً(٤٠).

الفرع الثاني: طرق الحماية والرقابة الأخرى.

---

(٣٩) شبكة النبأ المعلوماتية، الاثنين ٢٠٠٣/١٢/٢٥.

(٤٠) انظر:

www.maktoob.com/maktoob/press2002/apress2002-3.hotmail.

إن استخدام تكنولوجيا الجدران النارية تصنف ضمن وسائل " الرقابة المنطقية " للدخول إلى أنظمة وشبكة المعلومات الداخلية للمصرف (Logical Access Control) وهناك العديد من وسائل الرقابة المنطقية بالإضافة إلى وسائل الرقابة المادية (physical Access Control) يجب على المصرف المتعامل عبر الإنترنت إتباعها، لتوفير عنصر الأمان والرقابة السليمة للحفاظ على موجودات المصرف وسمعة الجهاز المصرفي بشكل عام، بعض هذه الوسائل اذكرها كما يلي :

- تشير مجموعة من الدراسات أن ما نسبه حوالي (٧٠%) من المهاجمين(Attackers) اللذين يحاولون الدخول والعبث بشبكة الموظفين العاملين لدى المصرف، حيث أن فرص المعرفة لديهم عن طبيعة الشبكة ونظم المعلومات الداخلية لديهم أعلى من المهاجمين من خارج المصرف، وعليه يجب على إدارة المصرف أن تحرص على توفير المعلومات عن الشبكة الداخلية وعن نظم المعلومات للموظفين المعنيين بذلك عند الحاجة فقط.
- استخدام نظام إلكتروني معقد لتكوين الكلمات السرية المقابلة لمفاتيح الدخول الإلكترونية (IDs)، حيث يجب أن تكون الكلمة السرية مكونة على الأقل من (٦-٨) خانات من الحروف والأرقام (Alphanumeric)، وأن يتم استحداثها بطريقة يصعب على أحد غير مستخدمها تخمينها، بحيث تكون سهلة الاستذكار من قبل مستخدمها ولكنها صعبة التخمين من قبل الغير، وفي هذا المجال يمكن الاستعانة بعلم الاستذكار

(Mnemonics) لتكوين كلمة دخول سرية (password)، فعلى سبيل المثال الكلمة السرية (أ خ ع بـ ت ٣٢١) صعبة التخمين إلا أنه يمكن لمستخدمها استذكارها من الجملة التي تقول (أمارات الخير والعطاء بلد التقدم) فإذا أخذنا الحروف الأولى من كل كلمة في الجملة بعد استثناء الـ التعريف وإضافة بغض الأعداد إليها نحصل على كلمة سرية سهلة الاستذكار من قبل المستخدم ولكنها صعبة التخمين من قبل الغير.

- يجب أن يقوم المصرف المتعامل عبر الإنترنت بتحديد وحصر كافة النقاط والأجهزة التي تربط شبكة وأنظمة معلوماته الداخلية مع الفضاء السايبيري الخارجي وأن يقوم بمراقبة هذه النقاط ومنع استخدام أية أجهزة أخرى من قبل الموظفين.
- يجب أن يقوم المصرف بكافة إجراءات الرقابة والحماية المادية (physical Security) للأجهزة، حيث يجب حفظ هذه الأجهزة في أماكن آمنة لا يسمح لأحد – غير الموظفين المخولين – بالدخول إليها.
- انتهاج أسلوب رقابة وتدقيق داخلي يتناسب مع طبيعة ومستوى خطورة وتعقيد العمل المصرفي عبر الإنترنت.

المطلب الثاني: الإجراءات المتخذة من قبل الحامل.

تتلخص الإجراءات التي يقوم بها الحامل، بعدد من الوسائل الوقائية التي تهدف إلى المحافظة إما على البطاقة من الضياع أو السرقة، أو المحافظة على الرقم

السري، حتى لا تقع البطاقة في يد غير صاحبها فيقوم باستخدامها استخداماً غير مشروع، وهذه الإجراءات هي:

١. أن يقوم الحامل بوضع البطاقة في مكان أمين، وأن لا يتركها في مكان تسهل فيه سرقتها، أو ضياعها.
٢. أن لا يقوم الحامل بإعطاء البطاقة إلى أي شخص حتى لو كان أحد أصوله أو فروعه، أو زوجه.
٣. أن لا يقوم الحامل بكتابة الرقم السري على جسم البطاقة، أو على ورقة منفصلة مع البطاقة، بل يجب عليه أن يحفظ الرقم السري غيباً، ويتلف الوثيقة التي يكون بها الرقم السري أو يحرقها.
٤. يجب على الحامل ألاّ يقوم بترديد رقمه السري أمام أي شخص، كذلك أنّ يحرص على أن لا يشاهده أحد وهو يقوم بإدخال الرقم السري في جهاز الصرّاف الآلي.
٥. يجب على الحامل أن لا يطلب الوصل المطبوع من جهاز الصرّاف الآلي، وان طلبه فإنّ عليه أن يقوم بأخذه لا بتركه، أو أن يقوم بإتلافه؛ لأنه يحوي على رقم حساب الحامل.
٦. يجب على الحامل ألا يرمي نسخة الفاتورة التي يعطيها التاجر له، بل عليه أن يحتفظ بها؛ لأنها تحوي على رقم البطاقة.
٧. يجب على الحامل عدم استخدام بطاقته لدى المحلات التجارية الصغيرة أو المطاعم المشكوك فيها.

٨. يجب على الحامل عند فقده لبطاقته، أو سرقتها إبلاغ المُصدر فوراً بواسطة الهاتف وفي أي وقت، حيث إن المُصدر قد وفر خدمة الاتصال به، وإبلاغه طوال (٢٤) ساعة في اليوم وسبعة أيام في الأسبوع، وبعد ذلك عليه أن يبلغ المُصدر خطياً.

٩. على الحامل عند الشك بأن رقم بطاقته، أو رقمها السري قد عُرف، أن يقوم بإبلاغ المُصدر فوراً والطلب منه إلغاء البطاقة.

١٠. أن يحرص الحامل على ألا يكون في حساب البطاقة إلا مبالغ قليلة حتى لا تكون الخسارة كبيرة أن تمّ السحب من الغير بواسطة البطاقة، وان يطلب من المُصدر بان لا يسمح له، أو للتاجر بتجاوز الرصيد، إلا أن قام هو بالاتصال بالمصدر، وقام بالطلب منه بعد أن يعطيه رمز التعريف الخاص به، حتى يتأكد المُصدر أن هذا الطلب كان من الحامل الشرعي للبطاقة.

ومن أهم الأشياء التي يجب على الحامل قبل إجراء أي عملية شراء، أو طلب خدمة عن طريق الإنترنت التأكد مما يلي:

١. وجود اتصال آمن (Secure Connection) وذلك بالتأكد من وجود كلمة https:// بدلاً من http:// في بداية عنوان الموقع، كما يمكن التأكد من ذلك بوجود القفل المغلق في أسفل نافذة المتصفح.

٢. موثوقية الموقع الذي يتعامل معه، فلا يعطي رقم البطاقة لمواقع صغيرة، أو غير معروفة ــ حتى أن كان الاتصال آمنا ــ بل يجب أن يكون التعامل مع المواقع المشهورة والموثوقة.

٣. لا ترسل معلومات شخصية عبر الشبكة مثل العنوان الشخصي، رقم الهاتف، رقم بطاقة الائتمان، رقم الضمان الاجتماعي، رقم البطاقة الشخصية، أو أية معلومات شخصية أخرى، إلا إذا كانت هذه المعلومات مرسلة باستخدام وسائل مشفرة.

٤. استخدام برامج كمبيوتر مشفرة مثل برنامج (PGP)(Pretty Good privacy) لضمان خصوصية البريد الإلكتروني (e-mail).و بعد إتمام العملية يطبع الصفحة التي تحتوي على مختصر للعملية التي قام بها[٤٠]،حتى يتمّكن من معرفة ما له وما عليه.

٥. عند وصول كشف حساب بطاقة الدفع الإلكتروني التأكد من جميع المبالغ التي تمّ تسجيلها على البطاقة، من أجل عدم وجود أي مبلغ من جهة لم يتعامل معها، وعند اكتشاف أي تلاعب لا بد من رفع شكوى إلى البنك الذي أصدر بطاقة الدفع الإلكتروني، وسيقوم المختصون هناك بالتحقق في ماهية الشخص، أو الجهة التي استخدمت بطاقة الدفع الإلكتروني دون تصريح من الحامل.

٦. المحافظة على كلمة السر وعدم حفظها على الجهاز وان لا يسمح للمتصفح بتذكرها، وكذلك أنّ يحرص على استخدام النسخ الحديثة من المتصفحات التي تمّ إصلاح الثغرات الأمنية فيها، وأن يحرص على أن يكون المتصفح يدعم التشفير بمفتاح طوله (١٢٨) بت، حتى تصعب المهمة على من يحاول كسر التشفير لغرض سرقة البيانات السرية.

---

(٤٠) أغلب المواقع تعرض هذه الصفحة على المستخدم كنوع من المراجعة قبل إتمّام العملية.

جرائم بطاقة الدفع الإلكتروني عبر شبكة الانترنت

قائمة المراجع

أولاً: المراجع العامة:

١. عبد الرزاق السنهوري، الوسيط في شرح القانون المدني الأردني، الجزء الثاني،المجلد الأول، رقم (٥٨)
٢. أحمد نشأت، رسالة الاثبات، الجزء الأول.
٣. عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإليكترونية، الكتاب الأول، نظام التجارة الإليكترونية وحمايتها مدنياً، دار الفكر الجامعي، الإسكندرية، جمهورية مصر العربية، الطبعة الأولى، ٢٠٠٢.

ثانياً: المراجع المتخصصة:

١. جميل عبد الباقي الصغير، الحماية الجنائية والمدنية لبطاقات الإئتمان الممغنطة "دراسة تطبيقية في القضاء الفرنسي والمصري"، دار النهضة العربية، القاهرة، جمهورية مصر العربية، ٢٠٠٣.
٢. محمد حسام محمد لطفي، استخدام وسائل الاتصال الحديثة في التفاوض على العقود وإبرامها، ١٩٩٣،بدون ناشر.
٣. عبدالفتاح بيومي حجازي،التوقيع الإليكتروني في النظم القانونية المقارنة،٢٠٠٥،ط١،دار الفكر الجامعي.
٤. سعيد السيد قنديل، التوقيع الإلكتروني، ٢٠٠٤، دار الجامعة الجديدة للنشر.

٥. عمر حسن المومني، التوقيع الإلكتروني وقانون التجارة الإلكترونية،٢٠٠٣، الطبعة الأولى، دار وائل للنشر والتوزيع.

٦. حسن الباسط جميعي، إثبات التصرفات القانونية التي يتم ابرامها عن طريق الإنترنت، الطبعة الأولى،دار النهضة، القاهرة، ٢٠٠٠.

٧. ثروت عبد الحميد، التوقيع الإلكتروني، ٢٠٠٢ – ٢٠٠٣، الطبعة الثانية، مكتبة البلاد الجديدة بالمنصورة.

٨. منير محمد الجنبيهي و ممدوح محمد الجبيهي، التوقيع الإلكتروني وحجيته في الإثبات، ٢٠٠٤،دار الفكر العربي.

٩. طوني ميشال عيسى: التنظيم القانوني لشبكة الإنترنت، دراسة مقارنة في ضوء القوانين الوضعية والاتفاقيات الدولية، المنشورات الحقوقية، صادر، بيروت، لبنان، الطبعة الأولى، ٢٠٠١.

١٠. حسين إبراهيم القضماني: البطاقة المصرفية والإنترنت، دراسة حول الوضعيتين التقنية والقانونية، مجلة اتحاد المصارف العربية، بيروت،الطبعة الأولى،٢٠٠٢.

١١. أروى فايز الفاعوري وإيناس محمد قطيشات، جريمة غسيل الأموال (المدلول العام والطبيعة القانونية)، دار وائل للنشر، عمّان، الأردن، الطبعة الأولى، ٢٠٠٢.

١٢. حسام العبد، غسيل الأموال الإلكتروني، مجلة البنوك في الأردن، العدد السابع، أيلول،٢٠٠٠، المجلد ١٩.

١٣. محسن الخضيري، غسيل الأموال "الظاهرة وأسباب العلاج"، مجموعة النيل العربية، القاهرة، جمهورية مصر العربية، ٢٠٠٣.

١٤. جلال محمدين، دور البنوك في مكافحة غسيل الأموال، دار الجامعة الجديدة للنشر، الإسكندرية، جمهورية مصر العربية، ٢٠٠٠.

١٥. سامح محمد عبد الحكم، الحماية الجنائية لبطاقات الإئتمان "جرائم بطاقات الدفع الإلكتروني"، دار النهضة العربية، القاهرة، جمهورية مصر العربية، ٢٠٠٣.

١٦. كيلاني عبد الراضي محمود: المسئولية عن الاستعمال غير المشروع لبطاقات الوفاء والضمان، دار النهضة العربية، القاهرة، جمهورية مصر العربية، ٢٠٠١.

ثالثاً: الرسائل الجامعية:

١. امجد حمدان الجهني، المسؤولية المدنية للاستخدام غير المشروع لبطاقة الوفاء ووضع الضوابط لذلك، رسالة دكتوراه، كلية الحقوق، جامعة عمان العربية للدراسات العليا،عمان،الأردن، ٢٠٠٥.

٢. كيلاني عبد الراضي محمود، النظام القانوني لبطاقات الوفاء والضمان، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، القاهرة، جمهورية مصر العربية ١٩٩٦، ص٧٣٩.

رابعاً: المؤتمرات والندوات:

١. أبو الوفا محمد أبو الوفا إبراهيم: المسئولية الجنائية عن الاستخدام غير المشروع لبطاقة الإئتمان، ورقة عمل مقدمة في مؤتمَّر الأعمال

المصرفية الإلكترونية بين الشريعة والقانون من ٩ – ١١ ربيع أول ١٤٢٤هـ. الموافق ١٠ – ١٢ أيار ٢٠٠٣م، كلية الشريعة والقانون/جامعة الإمارات العربية المتحدة وغرفة تجارة وصناعة دبي، دولة الإمارات، المجلد الخامس.

٢. نوري خاطر، بحث في وظائف التوقيع في القانون الخاص، منشور في مجلة المنارة، جامعة آل البيت مجلد ٣،عدد٢،١٩٩٨.

٣. الأستاذ المنصف قرطاس، حجية الإمضاء الإلكتروني أمام القضاء،بحث منشور في كتاب التجارة الإلكترونية والخدمات المصرفية والمالية عبر الإنترنت،اتحاد المصارف العربية.

٤. إبراهيم الدسوقي أبو الليل، بحث حول التوقيع الإلكتروني ومدى أهميته في الإثبات " دراسة مقارنة "، مؤتمر القانون والحاسوب، جامعة اليرموك، اربد الأردن ١٢– ١٤ تموز ٢٠٠٤.

٥. أيمن مساعدة، التوقيع الرقمي وجهات التوثيق، بحث مقدم لمؤتمر القانون والحاسوب ١٢ – ١٤ تموز ٢٠٠٤ جامعة اليرموك.

٦. عادل محمود مشرف عبد الله اسماعيل عبد الله. ضمانات الأمن والتأمين في شبكة الإنترنت،بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، الامارات العربية المتحدة،شهر ٥ /٢٠٠٠.

٧. عماد علي خليل: التكييف القانوني لإساءة استخدام البطاقات عبر شبكة الإنترنت. مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات العربية، العين، دولة الإمارات العربية المتحدة، ٢٠٠٠..

٨. علي حسني عباس، مخاطر بطاقات الدفع الإليكتروني عبر شبكة الإنترنت، المشاكل والحلول، ورقة عمل مقدمة في ندوة الصورة المستحدثة لجرائم بطاقات الدفع الإليكتروني، نظمت بمعرفة مركز بحوث الشرطة، أكاديمية الشرطة، القاهرة، جمهورية مصر العربية ١٤/١٢/١٩٩٨.

٩. أشرف توفيق شمس الدين، مدى ملاءمة تجريم غسيل الأموال للقواعد المصرفية، ورقة عمل مقدمة إلى مؤتمَّر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، نظمته جامعة الإمارات العربية المتحدة، ٩ – ١١/ربيع الأول/ ١٤٢٤هـ الموافق ١٠ – ١٢/٥/٢٠٠٣، المجلد الرابع.

١٠. زغلول محمود البلشي: مسئولية البنك الجنائية عن جرائم غسيل الأموال، ورقة عمل مقدمة إلى مؤتمَّر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، نظمته جامعة الإمارات العربية المتحدة، ٩ – ١١/ربيع الأول/ ١٤٢٤هـ الموافق ١٠ – ١٢/٥/٢٠٠٣،، المجلد الخامس.

سادساً:المراجع باللغات الأجنبية:

1. Sédaillan V., Droit de L'Internet. Collection AUI 1997. p.221.
2. Nguyen (H.), Des Paquts Cryptés Pour Sécuriser Le Paiement Sur Le Web, Le Monde Interactif (Le Monde Esition Proche – Oriect), 23 juin 2000,
3. Scott Seltzer, Money Laundering: The Scope of the Problem and Attempts to Combat.
4. Socio – Legal issues Affecting the use of Digital Signatures for secure E-Commerce Transactions: A caribberm perspective