الحماية العقدية للمستهلك في إطار وسائل الدفع الإلكترونية

ط.د زماموش نذير

كلية الحقوق - جامعة الجزائر 1 يوسف بن خدة

ملخص:

لموضوع وسائل الدفع بصفة عامة أهمية قانونية وعلمية في آن واحد، إذ تلعب هذه الوسائل دورا رئيسيا في جميع مناحي الحياة الاجتماعية، الاقتصادية والقانونية، ولعل العودة إلى النصوص العامة قد لا يكون كافيا لتغطية جميع المسائل المثارة أو التي يمكن أن تثار بشأن استعمال وسائل الدفع الإلكترونية ومن تم عدم وجود حماية كافية للمستهلك في هذا الصدد، وتبعا لهذا الواقع برزت مجموعة من الجهود التي تحاول فرض قواعد تنظيمية على عمل وسائل الدفع الالكترونية.

وهذه الجهود ليست واحدة موحدة في المعايير التي تفرضها، فإذا كانت جميعها ترمي إلى وضع حد أدنى من القيود على شروط العمل بوسائل الدفع هذه، بهدف تأمين أكبر قدر ممكن من الحماية للمستهلك، إلا أنها تبقي غير كافية مع التطور التكنولوجي المتسارع لمثل هذه الوسائل الإلكترونية في الوفاء.

الكلمات المفتاحية:

وسائل الدفع الإلكترونية، حرية التعاقد، الحماية العقدية للمستهلك

Résumé:

Les moyens de paiement ont en général une importance à la fois juridique et scientifique, car ils jouent un rôle essentiel dans tous les aspects de la vie sociale économique et juridique .Le retour aux textes généraux peut ne pas suffire à couvrir toutes les questions soulevées ou susceptibles de se poser concernant l'utilisation des moyens de paiement électroniques. Et le manque de protection adéquate des consommateurs à cet égard. En conséquence, un certain nombre d'efforts ont été déployés pour tenter de réglementer le fonctionnement des moyens de paiement électroniques.

Ces efforts ne sont pas uniformes dans leurs normes, si elles visent toutes à fixer des conditions minimales un travailler avec ces moyens de paiement, dans le but

de garantir le plus de protection possible au consommateur, mais ils restent insuffisants compte tenu du développement technologique rapide de tels moyens de paiement électroniques.

Mots clés :

Moyens de paiement électroniques- liberté contractuelle- protection contractuelle du consommateur.

مقدمة:

أصبحت جرائم وسائل الدفع الإلكترونية تمثل تهديدا مباشرا وفوريا وسريعا للاقتصاد العالمي والمحلي وحقوق الأفراد بغض النظر عن موقعهم من العالم، مما يتطلب تعاونا دوليا وإقليميا لمواجهة هذه النوعية المستحدثة من الجرائم وتضافر جهود كافة الأجهزة المعنية في الدولة وفي مقدمتها أجهزة الشرطة القضائية وأجهزة البحث العلمي والسلطة التشريعية حتى يمكن التصدي لتلك النوعية من الجرائم ولاشك أن التقدم العلمي بقدر ما أفاد جهات البحث والتحقيق وملاحقة الجرائم بقدر ما أفاد المجرمين أنفسهم فأصبحوا أكثر قدرة على التخفي وتضليل أجهزة العدالة والعبث بأدلة الاتهام.

وإذا كانت المسؤولية الجنائية عموما تعني الالتزام بالخضوع للأثر الذي ينص عليه القانون كجزاء على ارتكاب الجريمة وهو الخضوع للعقاب، فإن تجريم الاستعمال غير المشروع لوسائل الدفع الإلكترونية مازال قيد البحث وإن كان قد تم تطبيقه علي المستوي الدولي إلا أن التشريعات الداخلية لازالت قاصرة عن مواجهته وتأسيسا على ذلك نطرح التساؤل الآتي في غياب نظام قانوني خاص في التشريع الجزائري من شأنه الإلمام بكافة الإشكالات القانونية المثارة جراء الاستخدام غير المشروع لوسائل الدفع الإلكترونية هل تكفي القواعد الإجرائية المقررة في الجرائم التقليدية لكي تسري على الجرائم الإلكترونية؟

وسنحاول الإجابة عن هذه الإشكالية من خلال تقسيم موضوع مداخلتنا إلى ثلاث محاور: نتناول في المحور الأول الحماية في المجال التشريعي والقضائي على المستوي الدولي والداخلي، وفي المحور الثاني سنتطرق الحماية من الجانب الفني والتقني، لنصل في المحور الثالث للحماية في المجال الأمني.

المحور الأول: الحماية في المجال التشريعي والقضائي على المستوى الدولي والداخلي

أدى انعدام وجود تشريع عقابي واضح ومحدد لتجريم الأفعال غير المشروعة عن الاستخدام غير المشروع لوسائل الدفع الالكترونية إلى إثارة الجدل والتردد حول ما إذا كانت وسائل الدفع الالكترونية تعد محررا تنطبق عليه النصوص القانونية القائمة وفقا للتفسير الواسع للنص الجنائي وبين التمسك بمبدأ الشرعية الجنائية وما قد يتفرع عنه من خطر القياس في مواد التجريم والعقاب.

أولا : الحماية في المجال التشريعي:

سنستعرض فيما يلي نطاق الحماية في بعض الدول لبيان مدى مواجهتها لتلك النوعية من الجرائم المستحدثة.

أ-نطاق الحماية الجنائية في القانون الفرنسي:

نظرا للانتشار المتزايد للجرائم الواردة على وسائل الدفع الالكترونية[1] والتي من شأنها الإضرار بمصلحة حاملها أو ما يعرف بالمستهلك الإلكتروني[2] وتعدد وقائع الغش. رأى المشرع الفرنسي ضرورة التدخل التشريعي لكفاية حماية جنائية خاصة، فأصدر القانون رقم 19/88 المؤرخ في 05 جانفي 1988 الخاص بالغش المعلوماتي إلا انه لم يتناول الحماية الجنائية إلا بصفة جزئية وغير مباشرة في المادتين 462/ و 6/462 من قانون العقوبات الفرنسي الجديد وهاتان المادتان تتناولان تزوير المستندات المعالجة إلكترونيا واستعمالها.

وإزاء ضيق نصوص قانون العقوبات الفرنسي وعجزها عن كفالة تحقيق حماية جنائية كاملة لوسائل الدفع الإلكترونية وحسب الراجح في الفقه والقضاء الرافض لخضوع ومواجهة التزوير الذي يقع في مجال المعالجة الالكترونية للبيانات حسبما تقضي الأحكام العامة للتزوير في المحررات الخاصة في ظل المعطيات الإلكترونية الخاص بوسائل الدفع. يتضح لنا قصور الحمال الجنائية الخاصة لبطاقات الدفع الالكتروني في التشريع الفرنسي حيث اقتصرت على تجريم تزوير البطاقة واستعمالها أو قبولها مع العلم بتزويرها، ولم تمتد إلى حالة قيام حامل البطاقة باستخدامها على الرغم من انتهاء صلاحيتها أو إلغائها من جانب الهيئة التي أصدرتها، كما لا تمتد إلى حالة الاستخدام التعسفي على الرغم من عدم وجود رصيد دائن لحاملها لدى البنك كما لا تمتد هذه الحماية أيضا للغش الذي يصدر من حاملها عن طريق الإدعاء بفقدها أو سرقتها وتبليغ الجهة المصدرة لها بذلك تم يستمر هو في استخدامها في السحب أو الوفاء.

ب- نطاق الحماية الجنائية في القانون السويسري:

يجرم القانون السويسري في المادة 148 من قانون العقوبات الصادر في عام 1995 الاستخدام غير المشروع لبطاقات الدفع الالكتروني حيث تقضي هذه المادة بمعاقبة كل من يقوم

---

[1] عرفها المشرع في المادة 06 من قانون االتجارة الإلكترونية الجزائري رقم 18-05 ،المؤرخ في 10 ماي 2018 الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية العدد 28 ، المؤرخة في 16 ماي 2018.

[2] نفس المرجع السابق.

باستخدامها بطريقة غير مشروعة في الوفاء بقيمة السلع والخدمات وذلك إضرار بالجهة المصدرة أو المانحة لها، وخلافا للشروط المبرمة بينها وبين حاملها، كما جرمت المادة 148 في فقرتها الثانية استعمالها غير المشروع من قبل الغير حيث اعتبرت ذلك من قبل الاحتيال المعلوماتي[1].

ج-نطاق الحماية الجنائية في القانون الفنلندي:

يجرم قانون العقوبات الفنلندي في المادة الثامنة حتى الفصل السابع عشر من قانون العقوبات كل من يقوم لأجل الحصول ربح أو عائد مالي بدون وجه حق له أو للغير سواء باستعمال بطاقة بنكية أو ائتمانية أو شيك أو أية وسيلة سداد مشابهة دون موافقة مالكها الأصلي متجاوزا الحقوق المكفولة له دون حق شرعي ، أو دون تصريح من الجهة المانحة للبطاقة أو بالتجاوز للتصريح الممنوح من تلك الجهة وكذلك بنقل هذه البطاقة للغير لاستخدامها دون أن يكون له الحق قانونا في ذلك ويشير نص المادة صراحة على الحالات التي يتم الاستخدام غير الشرعي للبطاقة فيها مثل سحب ما يجاوز الرصيد أو ما يجاوز الحد الأقصى المسموح به كما عاقبت المادة التاسعة من ذات القانون مرتكب إنتاج أو تقليد وسائل السداد المزيفة باعتبارها جريمة احتيال[2].

د-نطاق الحماية الجنائية في التشريع الجزائري:

بالرجوع إلي المشرع الجزائري نجده قد تدارك الأمر نظر لأتساع نطاق استخدام وسائل الدفع الإلكترونية في العديد من المجالات من قبل حاملها أو ما يعرف بالمستهلك الالكتروني وظهور العديد من التجاوزات عليها، ما دفع المشرع إلي تعديل قانون العقوبات، ووضع عقوبات جزائية في حق الجناة مرتكبي الجرائم الالكترونية حيث أضاف فصلا سابعا تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات التي تتضمن المواد 394 مكرر إلي 394 مكرر 07 بموجب الأمر 04-15 المؤرخ في 17 نوفمبر 2004 ، ليأتي بعده مباشرة الأمر 05-06 المؤرخ في 23 أوت 2005 والمتعلق بمكافحة التهريب، الذي نص فيه المشرع صراحة في مادته الثالثة على وسائل الدفع الإلكترونية أين أعتبرها من بين الإجراءات والتدابير الوقائية التي تهدف إلي الحد من ظاهرة التهريب.

فضلا عن صدور المرسوم الرئاسي رقم 14-252 المؤرخ في 08 سبتمبر 2014 والمتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، التي تنص على ضرورة مكافحة جرائم الاستخدام غير المشروع لوسائل الدفع الإلكترونية.

---

[1] Roth robert, les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique en suisse , vol64,1993, p606.

[2] أيمن عبد الحفيظ، حماية بطاقات الدفع الالكتروني مطابع الشرطة للطباعة والنشر والتوزيع، القاهرة، مصر،2007، ص96.

مما تقدم تجدر الاشارة أنه رغم كل الجهود المبذولة سواء علي المستوي الداخلي او الدولي من طرف العديد من الدول من خلال إدراجها إلي نصوص قانونية تسعي جاهدة من ورائها إلي الحد من الجرائم الإلكترونية بإشكالها المختلفة سواء ما تعلق منها بوسائل الدفع الإلكتروني أو في حماية المتعاملين بمثل هاته الوسائل أو ما أطلق عليم مؤخرا باسم المستهلكين الإلكترونيين طبقا لنص المادة 06 من قانون التجارة الإلكترونية الجزائري رقم 18-05 المؤرخ في 10 ماي 2018 .

ثانيا: الحماية في المجال القضائي:

نجد أن ازدياد جرائم وسائل الدفع الالكترونية والتطور الرهيب والسريع نحو ارتكاب هذه الجرائم المستحدثة وخاصة الانتشار والازدياد المتلاحق في استخدام مثل هذه الوسائل الالكترونية المتاحة في الوفاء إما مباشرة أو عن بعد قد أدى إلى ظهور أنماط إجرامية لم تكن معروفة من قبل والتي قد يمتد نشاط لمعظم دول العالم، كون جل المعاملات تتم في فضاء افتراضي مفتوح، وعليه سنحاول الوقوف عند التكييف القانوني الملائم لبعض هذه الجرائم لحين إصدار التشريع المناسب أو إضافة النصوص التي تعالج هذه الجرائم.

أ-تطبيقات الحماية القضائية في فرنسا:

ذهبت محكمة استئناف ANGERS بفرنسا بحكم صادر لها "إلى أن استيلاء حامل البطاقة على مبالغ تتجاوز رصيده من خلال وضعها في أحد أجهزة الصرف الآلي المعد لذلك لا يشكل أي جريمة جنائية"

وقد أيدت محكمة النقض الفرنسية هذا الحكم عام 1982 حيث جاء في حيثيات حكمها أنه نظرا لأن محكمة الاستئناف ومن أجل الحكم ببراءة المتهم أثبتت أنه لكي يتمكن المتهم من إجراء السحوبات غير المشروعة فقد استخدم البطاقة بوصفه صاحبها وقد بررت محكمة الاستئناف حكمها بأنه الوقائع المنسوبة للمتهم تنطوي على عدم ملاحظة التزام تعاقدي ولا تندرج تحت أي نص جنائي[1].

ويرى البعض أن هذا الحكم فرق بين حالة قيام الحامل بإصدار شيك بدون رصيد وبين حالة قيامه بسحب مبالغ تتجاوز رصيده لدى البنك.

[1] مشار إليه عند: محمد سامي الشوا، ثورة المعلومات وانعكاساتها علي قانون العقوبات، الطبعة الثانية، دار النهضة العربية، القاهرة، مصر، 1998، ص125.

فالفعل الأول معاقب عليه والثاني لا يقع تحت طائلة التحريم مع أن كليهما أدوات وفاء وأنه كان من الأجدر على المشروع أن يفرق بينهما[1].

ب-تطبيقات الحماية القضائية في مصر:

عرضت إحدى القضايا أمام المحاكم المصرية، حيث تتلخص وقائعها في تحريك أحد البنوك جنحة مباشرة ضد أحد الأفراد بتهمة النصب المنصوص عليها في المادة 332 قانون عقوبات على سند من القول أن المدعى عليه تمكن من استخدام طرق احتيالية واستولى على مبلغ 7904.400 جنيه مصري و 99954 دولارا أمريكيا، وقال المدعى في صحيفة دعواه أنه بتاريخ 1983/6/30 استخرج المدعى عليه من البنك بطاقة دفع (فيزا كارد) وللحصول على هذه البطاقة قدم طلبا من البنك ادعى فيه أنه يعمل بدخل سنوي لا يقل عن 24000 جنيه، وتعهد بعدم استخراج هذه البطاقة ما لم يكن رصيده كافيا طبقا للعقد المبرم بينه وبين البنك، وبعد ذلك وعلى ما جاء بمذكرة ممثل البنك المدعى، يكون المدعي عليه قد تمكن من إيهام البنك بطرق احتيالية بأن رصيده في البنك سيكون كافيا لتغطية مصروفات مشترياته التي يحصل عليها من التاجر، ولكنه لم يقم بسداد ثمن المشتريات، فقام التاجر بالرجوع على البنك بوصفه ضامنا لحامل البطاقة، والذي قام بسداد ما على المدعى عليه من مديونيات[2].

وقد ذهب البعض في هذه الحالة إلى أنه إذا ثبت أن المعلومات التي أعطاها الحامل حول شخصيته غير صحيحة فإن المصدر يمكنه أن يحرك الدعوى الجنائية ضده، إذ أن هذه الأفعال وان كانت تدخل في النطاق التعاقدي بين العميل حامل البطاقة والبنك المصدر، إلا أنها تشكل جريمة جنائية[3]أما في هذه القضية فإن المدعى عليه قدم طلبا للبنك ادعى فيه أنه يعمل بدخل سنوي لا يقل عن 24000 جنيه.

وفي موضع آخر ذهب البعض في نفس القضية إلى أن المدعى عليه قدم مستندات تثبت أن دخله السنوي لا يقل 24000 جنيه، [4] والأمر هنا يختلف بين أن يدعي الشخص بأن دخله لا يقل عن 24000 جنيه وبين تقديم مستندات تثبت ذلك، فالادعاء لا يقام بشأنه جريمة تزوير، ولا يكون الأمر جريمة تقديم مستندات مزورة، وإنما يمكن أن يؤخذ وصف هذا "بالاحتيال" طبقا للمادة 336 ق ع، أما تقديم مستند يثبت دخله ويكون هذا المستند مزورا، فإنه تنطبق عليه جريمة التزوير بدون شك، طبقا لمادة 215 ق ع.

---

[1]هدى حامد قشقوش، الصورة الإجرامية لحالات السحب الإلكتروني من الرصيد، ورقة عمل مقدمة إلى ندوة " الصور المستحدثة لجرائم بطاقات الدفع الإلكتروني " ، أكاديمية الشرطة، مركز بحوث الشرطة، القاهرة، مصر، 1998، ص20.

[2]أيمن عبد الحفيظ، المرجع السابق، ص98.

[3]جميل عبد الباقي الصغير، الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة ، دراسة تطبيقية في القضاء الفرنسي والمصري ، دار النهضة العربية ، القاهرة ، مصر ، 2003، ص25.

[4]عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية، دار الفكر العربي، القاهرة، مصر، 2000، ص119.

ومما ثبت في هذه القضية أن المدعى عليه لم تتوافر في حقه أركان جريمة النصب، لذا قضت براءة المتهم استنادا إلى أن العلاقة بين المدعي (البنك) والمدعى عليه (الحامل) مجرد علاقة مدنية بحثه أساسها أن المدعى عليه بالحق المدني ضامن المدعى عليه بموجب البطاقة، وحيث أن البنك لا يعطي البطاقة للمدعى عليه، قبل أن يحصل على الضمانات الكافية، التي بموجبها يكون هو ضامن له، فإن البنك يتحمل هذه المسؤولية.

من خلال استعراضنا للنماذج التشريعية السابقة التي تناولت بالتجريم للأفعال غير المشروعة المتصلة بوسائل الدفع الإلكترونية نجدها كانت أكثر تركيزا على حماية هاته الوسائل المتاحة في الوفاء بغض النظر عن حماية حاملها وهو المستهلك الإلكتروني حيث نجد اختلافا فيما بينها في تحديد تلك الأفعال فاقتصرت بعض التشريعات على تجريم تقليد وتزوير هذه البطاقات دون التطرق إلى الاستخدام غير المشروع لوسيلة الدفع من قبل حاملها أو الغير.

المحور الثاني : الحماية في المجال التقني:

تتجلى حماية المعاملات المالية الإلكترونية في البطاقة البنكية التي تعتمد كوسيلة للوفاء الإلكتروني بالإضافة إلى ذلك هناك حافظة النقود الإلكترونية الافتراضية والتوقيع الالكتروني.

أولا :وسيط الوفاء الإلكتروني:

يتم عبر هذا الأسلوب نقل النقود من حساب المدين (العميل) لحساب الدائن (التاجر) ذلك بعد إتمام إجراءات الوفاء بين بنكي العميل والتاجر وقد كان من أبرز أنظمة التحويل بين الحسابات:

1-النظام الافتراضي الأولي: First Virtual

يقتضي هذا النظام أن يكون للتاجر حساب بنكي في بنك أمريكي وان يقوم العميل بتقديم المدين طلبا بفتح حساب لديها بعد أن يرسل لها خارج شبكة الإنترنت بالبريد العادي أو الهاتف رقم حسابه البنكي ورقم بطاقته البنكية الخاصة به بعد ذلك تقوم الشركة بتزويد العميل بمعرف Identifiant.

يقوم العميل بإرسال رقم تعريفه الشخصي للتاجر هذا الأخير الذي يستمع له بالتأكيد من وجود وكفاية حساب عملية لدى الشركة الوسيطة وذلك بأن يرسل لها معلومات الخاصة بالصفقة ورقم التعريف الشخصي للعميل والتاجر معاص تم ترسل هذه الشركة للعميل الذي يتطابق مع المعرف (الهوية) رسالة إلكترونية تطلب منه تأكيد عملية التسوية فتقوم الشركة الوسيطة بعد حصولها على رضا العميل بإرسال كامل المعلومات عبر شبكة البنوك التقليدية التي يتم من خلالها تنفيذ عملية تحويل النقود من حسبا العميل لحساب الشركة الوسيطة وليس لهذه الشركة بعد ذلك غير الوفاء بالنقود للتاجر وإخطاره بنجاح عملية الوفاء حتى يتمكن من تنفيذ التزامه تجاه العميل.

2- نظام : "kleline"

وعلى خلاف النظام السابق يحتاج العميل المستفيد من نظام "kleline" إلى ان يضيف إلى حسابه الإلكتروني الشخصي برنامج للوفاء الأمن يسمى (Kleline) وبعد أن يرسل العميل طلب شراء بضاعة معينة إلى التاجر يرسل هذا الأخير بطاقة وفاء إلكتروني إلى الشركة الوسيطة التي يجب عليها بعد الإستيثاق من التاجر الذي ترسل بطاقة الوفاء إلى العميل.

وبعد استلامه لهذه البطاقة على العميل أن يصدر قبوله لها إلكترونيا وبعد رضا العميل تقوم "Kleline" بإتمام عملية الوفاء وتضع تحت تصرف التاجر قسيمة صندوق (Bonde caisse).

وبالرغم من الميزة الأساسية لنظام Kleline الذي يتمثل ضمان الأمان لعملية الوفاء عبر برنامج حاسوبي خاص وضمان الوجود الفعلي للتاجر الذي يجب أن يكون مسجلا لدى الشركة فإنه له مجموعة من السلبيات متمثلة:

- كون هذا النظام خاص بالتجار الفرنسي فهو ليس عالميا كغيره من الأنظمة مع أن هذا النظام يبقى مفتوحا للمستهلكين الأجانب حيث يسمح برنامج الوفاء الآمن (Kleline) بتنفيذ شراء بعملات مختلفة.

- أي الوفاء إذا تم عن طريق(المحافظ الافتراضية فيجب على العميل أن يفتح محفظة لكل تاجر يتعامل معه ، ولا يستطيع أن يستعمل هذه المحفظة إلا بالنسبة لهذا التاجر وحده فإذا تم الوفاء بواسطة البطاقة البنكية فلا حاجة للتوقيع الإلكتروني ف للعميل مما يوفر فرصة للغش.

- يعد هذا النظام من التعقيد بمكان بحيث عادة ما يكون مكلفا للتجار ولا يشجع المشروعات الصغيرة والمتوسطة على استخدامه.

إلا أنه بالرغم ما تحمله هذه الطريقة (وسيط الوفاء الإلكتروني) من تقليل لمخاطر الوفاء الإلكتروني فقد أخذ عليها أنها لا تساعد تطوير التجارة الإلكترونية حيث تدخل وسيط بين المتعاقدين يعد أمرا غير مرغوب من جانب المورد أو من جانب عملائه[1].

ثانيا: حافظة النقود الإلكترونية والافتراضية :

ويقصد بهذه التقنية تجميع وحدات للقيمة وذلك في أداة مستقلة عن الحسابات البنكية فظهرت بذلك فكرتي حافظة النقود الإلكترونية PME[2] وحافظة النقود الافتراضية PMV[3] فبالنسبة للأولى فإنها تشحن مسبقا برصيد مالي ويتم تسجيل هذا الرصيد المالي في بطاقة أما بالنسبة لحافظة النقود الافتراضية فإنها تشحن برصيد مالي على القرص الصلب لجهاز الكمبيوتر

[1] عبارة عن رقم تعريف شخصي يرسل بالبريد ليستعمله أثناء عملية التسوية (أورده ضياء علي أحمد نعمان بمقاله المعنون بالحماية التقنية للتجارة الإلكترونية الصادر بمجلة قانون وأعمال مجلة قانونية متخصصة ،العدد الأول 2011 ،مطبعة والوراقة الوطنية، مراكش ،ص20.

[2] حافظة النقود الإلكترونية PME: porte mammaire électronique.

[3] حافظة النقود الافتراضيةPMV porte monnaie Virtual .

الخاص الذي يستعمل الشبكة وبالتالي فقطع النقود أو النقود الافتراضية تمثل من الناحية الفنية تلك المعاملات المختزلة على ذاكرة جهاز الكمبيوتر ويستطيع بذلك العميل الذي يرغب في التعامل بهذه النقود أن يحصل من أحد البنوك أو أحد المؤسسات الوسيطة على رخصة تسمح له باستعمال النقود الإلكترونية بالمقابل الذي يتفق عليه ويكون بدءا مفتاح عام وخاص من أجل تأمين معاملاته وتحققها[1].

والهدف من هذه التقنية : تفادي اختراق البيانات التي يتم تداولها عبر شبكة الإنترنت والتغلب على إمكان استخدامها بين المشروع من قبل الغير. لأنه بهذه التقنية يصبح لوحدات القيمة الإلكترونية ذاتية مستقلة حيث يمكن نقلها من محفظة إلكترونية إلى أخرى نحو يؤدي إلى الوفاء من قبل المدين بمجرد فقل هذه الرموز الإلكترونية ويمكن لمتلقي هذه الوفاء على حافظة إلكترونية أن يقوم بتحويل هذه النقود الإلكترونية إلى نقود رقمية من خلال البنك المصدر لها.

ومن سلبيات هذه التقنية : فرض عمولات كبيرة على البنوك المتعاملة بهذا النظام مقابل تحويلات النقود الإلكترونية إلى نقود حقيقية ، كما أن تطور نظام النقد الإلكتروني ينطوي على تهديدي لاحتكار المركزية عملية إصدار النقود.

كما أن عدم إمكانية تتبع العمليات التي تتم من خلال النقود الإلكترونية يخشى منه ازدياد فرص التهرب الضريبي وربما يفتح بابا جديدا لعمليات غسل الأموال كما أن استخدام هذه التقنية لا يخلوا من مخاطر فنية متمثلة في إمكانية تعطل القرص الصلب وضياع ما عليه من مبالغ نقدية الكترونية[2].

ثالثا: التوقيع الإلكتروني:

إن المشرع الجزائري قد نص صراحة على التوقيع الإلكتروني بموجب القانون رقم 05-10 المعدل والمتمم للقانون المدني في نص المواد 327 ف01 و323 مكرر 1 [3]. وبهذا نجده نص صراحة على أن يكون للتوقيع الإلكتروني نفس حجية التوقيع التقليدي في الإثبات بشرط التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامته. لكنه لم يتوقف عند هذا الحد لينص عليه مرة أخرى في المادة 03 مكرر من المرسوم التنفيذي رقم 16207 المؤرخ في 30 ماي 2007 المتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية، وعلى مختلف خدمات المواصلات السلكية

[1] عبد الرحيم بن بوعيدة وضياء علي أحمد نعمان، موسوعة التشريعات الإلكترونية المدنية والجنائية مطبعة ووراقة الوطنية مراكش الجزء الثاني ،طبعة 2010، ص 24 .

[2] هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت دار النهضة العربية الإسكندرية القاهرة طبعة 1992 ص61.

[3] أضيفت بالقانون رقم 05-10 المؤرخ في 20 يونيو 2005 ج. ر 44- ص 24.

واللاسلكية[1].اعتبر أن التوقيع الإلكتروني ينجم عن استخدام أسلوب عمل يستجيب للشروط المحددة في المادتين 323 مكرر و323 مكرر01. غير أن المشرع لم يعرف التوقيع الإلكتروني من خلال هذا المرسوم.

وظل الأمر على حاله إلى غاية 2015 حيث أصدر قانونا خاصا بالتوقيع الالكتروني حاول من خلاله إيجاد الحلول لجميع الإشكالات القانونية التي قد تطرأ في المستقبل في ظل تبلور وتطور المعاملات والمبادلات الإلكترونية. وهو القانون رقم 15-04 المؤرخ في 01 فيفري 2015 الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين. ويؤكد فيه المشرع على ضرورة اعتماده في جميع الخدمات الالكترونية من خلال وضعه لهيئات خاصة بالتصديق الإلكتروني التي من شأنها خلق نوع من الثقة في مثل هذه المعاملات، حيث تعهد لها مهمة ترقية استعمال التوقيع والتصديق الإلكترونيين وتطويرهما وضمان الثقة في استعمالهما.

بهذا يكون المشرع الجزائري قد خطى خطوة جد مهمة في اعتماده للتوقيع الإلكتروني في إثبات التعاملات الإلكترونية خصوصا وسائل الدفع الإلكترونية والتي هي الأخرى بحاجة إلى قانون خاص ينظمها لخلق نوع من الثقة لدى المتعاملين بها.

رابعا: حماية مواقع الإنترنت :

تتجلى حماية المواقع الخاصة بالإنترنت ممن خلال نظام التشفير ،بالإضافة إلى الجدران النارية.

أ- نظام التشفير (كوسيلة لحماية سرية المعلومات):

التشفير هو إجراء يؤدي إلى توفير الثقة في المعاملات الإلكترونية وذلك باستخدام أدوات ووسائل تحويل المعلومات بهدف إخفاء محتواها والحيلولة دون تعديلها أ استخدامها المشروع. وقد عرفه المشرع المغربي في القانون رقم 53.05 من القانون المتعلق بالتبادل الإلكتروني للمعطيات القانونية في نص الفقرة الثانية من المادة 12 "بأنه كل عتاد أو برمجة أو هما معا ينشأ أو يعدل من أجل تحويل معطيات سواء كانت عبارة عن معلومات أو شعارات أو رموز استنادا إلى اتفاقيات سرية أو من أجل إنجاز عملية عكسية لذلك بموجب اتفاقية سرية أو بدونها".

ويعرف كذلك التشفير بأنه عملية تحويل المعلومات إلى رموز غير مفهومة تبدو غير ذات معنى بحيث يمنع الأشخاص غير المرخص لهم من الاضطلاع على المعلومة أو فهمها فعملية

[1]المرسوم التنفيذي رقم 07-162 المؤرخ في 30 مايو 2007 يعدل و يتمم المرسوم التنفيذي رقم 01-123 المؤرخ في 09 مايو 2001 المتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية على مختلف خدمات المواصلات السلكية واللاسلكية، ج ر، العدد 37 المؤرخ في 07 يونيو 2007، ص 13.

التشفير تنطوي على تحويل النصوص العادية أو نصوص مشفرة ومن المعلوم أن الإنترنت تشكل الوسيط الأضخم لنقل المعلومات ولابد من نقل المعلومات الحساسة لحركات المالية والتواقيع الإلكترونية بصيغة مشفرة إن أريد الحفاظ على سلامتها من عبث القراصنة.

ويسمح نظام التشفير بتلافي بعض المخاطر المتوقعة من استخدام الطرق الإلكترونية في المعاملات التجارية حيث يتم التأكد من طريقة من أن المعلومات التي تسلمها المرسل إليه هي تلك البيانات التي قام المرسل بالتوقيع عليها ، فالتشفير يساعد على حفظ سرية المعلومات والتوقيع الإلكتروني الذي يتطلب الحفاظ على الأرقام والرموز لحمايته داخل التجارة الإلكترونية.

والغاية من التشفير هو إيجاد وسيلة للمحافظة على سرية البيانات وحمايتها لكي لا يستطيع أي شخص الاضطلاع على هذه البيانات غير المتعاقدين أو من يصرح له قانونا بذلك كما يهدف التشفير إلى منع الغير من التقاط الرسائل أو المعلومات ومن تم منع وصولها مشوهة للطرف الآخر في المعاملات التجارية على نحو يعرقلها.

وهو نوعان (التشفير):

1-نظام التشفير المتماثل أو المتناظر:

وهو أسلوب من أساليب التشفير يستخدم فيه مفتاح سري لتشفير رسالة ما وفك تشفيرها ويسمى بالمفتاح المتناظر لأن المفتاح الذي يستخدم لتشفير الرسالة هو نفسه المستخدم لفك تشفيرها ، لكن هذه الطريقة تتطلب إحالة المفتاح بين الأطراف بطريقة يجب أن تضمن سلامته وتعطي هذه التقنية حماية أكثر في الشبكة المغلقة.

2-نظام التشفير اللامتماثل و اللامتناظر :

وهو أسلوب من أساليب التشفير يتم فيه تشفير البيانات باستخدام مفتاح ما وفك تشفيرها باستخدام مفتاح آخر ولهذا السبب يسمى بالتشفير بالمفتاح اللامتناظر لي مفتاح التشفير يختلف عن مفتاح فك التشفير وهكذا الفرق بين التشفير المتناظر والتشفير اللامتناظر بسيط جدا وكله غاية في الأهمية على مستوى ودرجة الأمن حيث أنه في التشفير المتناظر يتم تشفير الرسالة أو التوقيع باستخدام الرقم العام وفي نفس الوقت يتم فك الشفرة وإرجاع المعلومات إلى وضعها الأصلي باستخدام نفس الرقم العام ولو حصل أن شخص آخر يعرف هذا الرقم أو توصل إليه عن طريق الدليل العام فبإمكانه فك الشفرة وقراءة الرسالة أو التوقيع. أما إذا تم تشفير المعلومات بأسلوب التشفير اللا متناظر فإن المعلومات يتم تشفيرها بالرقم العام ولكن لا يمكن فك الشفرة والوصول إلى تلك المعلومات إلا بالمفتاح الخاص لصاحب ذلك المفتاح العام الذي تم على أساسه التشفير.

وفي هذا الإطار والهدف تأمين سلامة الاتصالات وعلى الأخص في التجارة الإلكترونية فقد أصدرت فرنسا أربعة مراسيم وستة قرارات تطبيقية لها خاصة بأنظمة التشفير ضمن حلول تعديل المادة 28 من قانون 29 ديسمبر 1990 قام القانون الصادر بتاريخ 26 جويلية 1996 بتحريري الاستعمال الشخصي لوسائل وخدمات التشفير التي لها وظيفة التوثيق وضمان وحدة

البيانات بالإضافة إلى تلك التي لها وظائف تأمين السرية ولا تستعمل إلا من خلال اتفاقات سرية منظمة من قبل مؤسسات معتمدة لكن عندما تؤمن خدمات التشفير وظائف المحافظة على السرية باستعمال مفاتيح ليست منظمة من طرف الغير ذوي الثقة فإن الاستعمال الشخصي لوسائل وخدمات التشفير التي لها وظيفة التوثيق وضمان وحدة البيانات بالإضافة إلى تلك التي لها وظائف تأمين السرية ولا تستعمل إلا من خلال اتفاقات سرية منظمة من قبل مؤسسات معتمدة من طرف الغير ذوي الثقة فإن الاستعمال الشخصي لهذه الوسائل والخدمات يكون خاضعا لترخيص صادر عن السلطة الحكومية العليا. بالنسبة لمستويات التشفير أصبح يستعمل ويستخدم أكثر من مستوى من أجل تحقيق أعلى درجة من الأمان فعلى سبيل المثال أصبحت المعاملات المالية الآن يتم تشفيرها باستخدام نظام تأمين المعاملات الإلكترونية SET[1] بالإضافة إلى تشفير لمستوى التصفح باستخدام net escape للتأمين SSl[2].

2-1- نظام المعاملات الإلكترونية الآمنة set

وهو يعد أهم برتوكول متعلق بالنواحي التأمينية وهدفه الأساسي هو تأمين عملية الوفاء والمعاملات المالية التي تتم أثناء المعاملة التجارية.

ويتميز هذا النظام عن الأنظمة التأمينية الأخرى بعدة مميزات كونه:

- يضمن أن طلب الشراء المرسل هو نفسه الطلب الذي يستقبله صاحب المشروع أو التاجر عن طريق بصمة ورقية معينة تكون مميزة لهذا الطلب.

- يضمن سرية طلب الشراء عن طريق تشفير المعلومات التي يشملها الطلب وكذلك البيانات الخاصة بعمليات الوفاء.

- يضمن للتاجر أو صاحب المشروع أن حامل البطاقة البنكية هو الشخص نفسه الذي يزعم هو عن طريق الشهادة التي يحملها والصادرة عن البنك الضامن أو شركة الائتمان الضامنة له والتي تؤكد لصاحب المشروع أو التاجر أن هذا الشخص الراغب في الشراء هو نفسه صاحب رقم الحساب المذكور كما أنه يعطي للتاجر ضمان بأن حساب المشتري يسمح بشراء هذه السلعة أو الخدمة المراد شرائها دون معرفة البائع برقم البطاقة البنكية الخاصة بالمشتري.

2-2- نظام للتأمين SSL

وتكمن مهمة البرتوكول في تشفير جميع الاتصالات حين أحد برامج التصفح أو النوافذ على شبكة المعلومات (Bowser) وأحد المواقع أو أحد مقار المعلومات على خادم الشبكة (Server) وبالتالي فهو يقلل من فرصة وقوع المعلومات أثناء عملية انتقالها في أيدي أي شخص غير مرغوب فيه إلى أن تصل إلى المستقبل النهائي فهو يعطي للعملاء الثقة والطمأنينة بأن

---

[1] SET : secure electronic transaction

[2] SSL : secure socket layer

المعلومات والبيانات الخاصة بهم بما فيها إتمام البطاقات البنكية لن تكون متاحة سوى للتاجر أو المنشأ أو المؤسسة المراد التعامل معها ...للتأمين البطاقة البنكية) .

ب-الجدران النارية (كوسيلة لحماية المحتوى):

يعتبر الجدار الناري وسيلة تستعمل لحماية الشبكات الخاصة من الدخول وتمنع الوصول الغير مشروع به للشبكة حيث تحمي وحدات التحكم والإرسال في الإنترنت.

وتتجلى أهمية الجدران النارية في حماية الشبكات الخاصة من هذه المشكلات حيث اف الإنترنت نتعامل على بث متعدد الأطراف باستعمال الأجهزة السمعية والبصرية ومؤتمرات الفيديو لمجموعة من المضيفين ليرى ويسمع كل منهم الآخر ويوفر الهيكل الإذاعي المتكامل على الإنترنت عن طريق برنامج (Mphone) المتوافر لكل الناس حيث أن أي مستعمل في الإنترنت يستعمل في هذا الجهاز (Mphone) يتيح المجال لأي مستعمل آخر للدخول عليه ومراقبته في الإنترنت ولكن الجدران الناري يعد هذا الدخول.

وتظهر مزايا وعيوب هذه الجدران النارية فيما يلي :

***بالنسبة لمزاياه :** توفير الحماية اللازمة للشبكة والمعلومات والحد من تعرضها للأخطار ومتابعة المستخدمين للشبكة ومن يحاول العبث بها.

- تسجيل وقائع الاستخدام بدقة طالما أن كل الرسائل والأوامر تمر به عند خروجها إلى الإنترنت أو قدومها منها.

- تسجيل كافة المعلومات عن حركة المرور هذه.

***أما عيوبه** فتتجلى في: عدم تعامله مع تنفيذ البرامج الداخلية التي تهاجم النظام فمادام موقع جدران الحماية هو على حدود الشبكة فإنه لا يستطيع أن يفعل الكثير لمهاجم من الداخل يريد سرقة بعض المعلومات من أحد أجهزة الشبكة الداخلية أو تخريب الأجهزة أو البرامج أو تعديلها:

- عدم توفير حماية قصوى وفورية باعتبار أن الجدران الناري يجب القيام بتحديث تهيئته باستمرار لمواكبة ما يتم اكتشافه من أحكام جديدة.

- استخدام الجدران النارية لموقع خاص بأحد المشروعات غير كافي لحماية الوفاء الإلكتروني بالبطاقات البنكية التي تتم داخل الموقع وبالتالي يتم الاستعانة بأحد البرتوكولان SSL، SET لضمان تأمين المعاملات أثناء العملية التجارية[1].

[1] ضياء علي أحمد نعمان ، المرجع السابق، ص39.

المحور الثالث: الحماية في المجال الأمني:

تواجه الأجهزة الأمنية اليوم تحديا جديدا أو كعادتها دائما فقد بدأت في مواجهة هذا التحدي وتلك الظاهرة منذ نشوئها، وذلك نظرا لانعدام وجود تشريع عقابي لتجريم بعض الأفعال الغير مشروعة المصاحبة لهذا النوع من الإجرام الحديث.

ويتركز الدور الأمني في مواجهة جرائم إساءة استخدام وسائل الدفع الإلكتروني في أسلوب التأمين من حيث منع وقوعها وكيفية تعاملها مع الأدلة المتحصل منها في حالة وقوعها. حيث يقع على الأجهزة الأمنية[1] العبء الأكبر في الحد من ارتكاب هذه الجرائم قصد حماية حاملها أو ما يعرف بالمستهلك الإلكتروني وهو ما يتطلب بدوره العمل على تحقيق ما يلي:

التنسيق والتعاون بين الأجهزة الأمنية والبنوك المصدرة لتلك الوسائل الإلكترونية في الوفاء وتبادل الاتصال والمعلومات حول هذه النوعية من الجرائم لسرعة ضبطها واكتشافها واتخاذ الإجراءات القانونية الفورية حيال مرتكبيها.

إنشاء قاعدة بيانات تتضمن كافة المعلومات عن قضايا وسائل الدفع الإلكترونية سواء على المستوى الوطني أو الدولي للتعرف على حركة وأبعاد الجريمة باعتبارها جريمة دولية أي ليس لها موطن محدد.

إنشاء إدارة متخصصة بجرائم وسائل الدفع الإلكترونية تتبع إدارة البحث والتحريات وذلك منعا للتخصص في تلك النوعية من الجرائم وما شهدته من تطور وازدياد في الفترة الأخيرة.

دعم التعاون الدولي والإقليمي بين الأجهزة الأمنية في مجال مكافحة جرائم وسائل الدفع الإلكترونية لتبادل المعلومات والخبرات خاصة في ظل حرص الدولة على تشجيع الاستثمار وجذب السياحة من خلال التنسيق مع منظمة الشرطة الجنائية الدولية (الإنتربول) لدراسة مدى إمكان إقرار تنظيم أمني دولي يكفل حماية المجتمع الدولي من مخاطر وسائل الدفع.

تدريب كوادر على أحدث الوسائل العلنية للكشف عن الجرائم المستحدثة من خلال التنسيق والتعاون مع المنظمتين الدوليتين (الفيزا، الماستركارد) للاستفادة من الخبرات الواسعة التي يتمتع بها ممثلون ولخبراتهم في التعرف على أساليب التزوير والاحتيال وأحدث الوسائل اللازمة لمواجهتها.

[1] أيمن عبد الحفيظ، المرجع السابق، 120.

خاتمة :

من خلال هذه الدراسة، يتبين أن المشكلة الحقيقية لدى المتعاملين بالوسائل الحديثة للدفع الإلكتروني تكمن في عدم قدرة القانون على مسايرة ما تشهده التكنولوجيا المتقدمة من تطورات، ذلك أن القانون لا يتطور بنفس السرعة التي تتطور بها التكنولوجيا الحديثة مما ستولد معه بالتالي العديد من الثغرات القانونية التي سبقت الإشارة إليها، سواء تعلق الأمر بالتكييف القانوني للأفعال المتأتية في سبيل استعمال هذه الوسائل، أم تعلق الأمر بالاختصاص القضائي أو الإثبات، سواء على مستوى إثبات هوية العميل أم على مستوى العمليات التي تنتج عنها.

لذا لابد من ضرورة الاندماج في ظل العولمة الاقتصادية العالمية، الذي يتطلب الأخذ بأسباب التقدم التقني على مستوى تبادل السلع والخدمات والأموال، ويقتضي ذلك بدوره العمل على عولمة القاعدة القانونية لمسايرة المتغيرات التي أحدثتها تكنولوجيا المعلومات في مجال إتمام التصرفات القانونية التي تتم من خلال وسائل الدفع الحديثة، وبالتالي يستوجب على التشريعات العربية التي من بينها الجزائر، العمل على إجراء التعديلات والتغيرات وسن القوانين الحديثة لإزالة كل العقبات القانونية التي تحدثها عملية استخدام المعلومات من حيث سلامة بياناتها وصحة توثيقها وتأمين عملية الدفع بموجبها. وفي إطار الجرائم المستحدثة نجد عدم وجود قانون خاص بوسائل الدفع الالكترونية خاصة وأن هذه الوسائل تعتمد على ثالوث عقدي أصبح في بعض جوانبه لا يساير القواعد العامة الموجودة في القانون المدني، والتي لم تعد كافية للإحاطة بجميع الجوانب المتعلقة بوسائل الدفع الإلكترونية سواء العقدية أو تلك المتعلقة بالمسؤولية، وكذا عدم مواكبة النظام العقابي الجزائري للجرائم المستحدثة بهذه الوسائل، وهذا يعتبر المشكل الرئيسي لإحجام سواء التجار أو المستهلكين التعامل بهذه الوسائل.

التوصيات :

نظرا لغياب التأطير التشريعي لهذا المجال ، ونظرا لأهميته المتنامية فإنه يجدر بالمشرع الجزائري وضع تقنين خاص ومفصل ينظم ويحكم جميع الجوانب القانونية والتنظيمية لنظام الدفع الإلكتروني ، بما يكفل الحماية القانونية للمتعاملين بها ، ويعالج المشكلات المالية المتوقع حدوثها في المستقبل من خلال الاستفادة من خبرات دولة سباقة في هذا المجال مع تجنب الأخطاء التي وقعت فيها .

إيجاد نوع من التنسيق والتعاون بين البنوك العاملة في هذا المجال وتبادل المعلومات الخاصة بالعملاء والتجار ذوي السمعة السيئة مع إفساح المجال للتنافس بين البنوك بهدف الوصول إلى أفضل خدمة لوسائل الدفع الإلكترونية بأقل عمولة وتكلفة.

ضرورة إنشاء هيئة خاصة لواجهة الجرائم الإلكترونية بأشكالها المختلفة لرصد ودراسة كل ما يتعلق بهذه الجرائم للعمل على كيفية مواجهتها مصرفيا والحد من تكرارها .

الاستمرار في عقد المؤتمرات والندوات الخاصة بمكافحة جرائم الاستخدام غير المشروع لوسائل الدفع الإلكترونية.

ضرورة إدخال مادة مكافحة الجرائم المستحدثة والتي من بينها مكافحة الجرائم المعلوماتية ومكافحة جرائم بطاقات الدفع الإلكتروني ضمن البرامج والمواد التي تدرس بأكاديمية الشرطة.

الحاجة إلى تعاون دولي حقيقي في ميدان أنشطة التحري والتحقيق والضبط والتفتيش خارج الحدود ، فلابد من المواجهة الحاسمة لجرائم الاستخدام غير المشروع لوسائل الدفع الإلكترونية بمختلف أنواعها وأشكالها ، كونها تحدث نتيجة استخدام خبرات مصرفية وقانونية وتقنية ، لذلك فإن مواجهتها تحتاج لنفس الخبرات ، مع محاولة التوصل إلى صيغة موحدة لاتفاقيات دولية تشمل الجوانب القانونية والتقنية للتعاملات المصرفية الإلكترونية حتى تتماشى والنظام الداخلي للدول.

تشجيع الباحثين على الكتابة والبحث في هذا الموضوع لما يوفره من معطيات ومعارف قانونية تسهل العمل التشريعي والقضائي ، مع منحهم الفرصة لإجراء تربص على مستوى البنوك والمؤسسات المالية لتوسيع معارفهم في الجانب العملي .

قائمة المصادر والمراجع:

أولا : قائمة المصادر:

1. القانون رقم 05-10 المؤرخ في 20 يونيو 2005 ج. ر 44، ص 24، يعدل ويتمم الأمر رقم 75-58 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975 والمتضمن القانون المدني، المعدل والمتمم.

2. المرسوم التنفيذي رقم 07-162 المؤرخ في 30 مايو 2007 يعدل و يتمم المرسوم التنفيذي رقم 01-123 المؤرخ في 09 مايو 2001 المتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية على مختلف خدمات المواصلات السلكية واللاسلكية، ج ر، العدد 37 المؤرخ في 07 يونيو 2007، ص 13.

3. قانون التجارة الإلكترونية الجزائري رقم 18-05 ،المؤرخ في 10 ماي 2018 الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية العدد 28 ، المؤرخة في 16 ماي 2018.

ثانيا: قائمة المراجع:

1. أيمن عبد الحفيظ، حماية بطاقات الدفع الالكتروني مطابع الشرطة للطباعة والنشر والتوزيع، القاهرة، مصر،2007.

2. عبارة عن رقم تعريف شخصي يرسل بالبريد ليستعمله أثناء عملية التسوية (أورده ضياء علي أحمد نعمان بمقاله المعنون بالحماية التقنية للتجارة الإلكترونية الصادر بمجلة قانون وأعمال مجلة قانونية متخصصة ،العدد الأول 2011 ،مطبعة والوراقة الوطنية، مراكش .

3. جميل عبد الباقي الصغير، الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة ، دراسة تطبيقية في القضاء الفرنسي والمصري ، دار النهضة العربية ، القاهرة ، مصر ، 2003.

4. عبد الرحيم بن بوعيدة وضياء علي أحمد نعمان، موسوعة التشريعات الإلكترونية المدنية والجنائية مطبعة ووراقة الوطنية مراكش الجزء الثاني ،طبعة 2010.

5. عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية، دار الفكر العربي، القاهرة، مصر، 2000.

6. مشار إليه عند: محمد سامي الشوا، ثورة المعلومات وانعكاساتها علي قانون العقوبات، الطبعة الثانية، دار النهضة العربية، القاهرة، مصر، 1998.

7. هدى حامد قشقوش، الصورة الإجرامية لحالات السحب الإلكتروني من الرصيد، ورقة عمل مقدمة إلى ندوة " الصور المستحدثة لجرائم بطاقات الدفع الإلكتروني " ، أكاديمية الشرطة، مركز بحوث الشرطة، القاهرة، مصر، 1998.

8. هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت دار النهضة العربية الإسكندرية ،القاهرة ،طبعة 1992.

9. حافظة النقود الإلكترونية PME: porte mammaire électronique.

10. حافظة النقود الافتراضيةPMV porte monnaie Virtual

11. Roth robert, les crimes informatiques et d’autres crimes dans le domaine de la technologie informatique en suisse , vol64,1993, p606.

12. SET : secure electronic transaction

13. SSL : secure socket layer