

وسائل الدفع ما بين الحماية التقنية والقانونية

للمستهلك الإلكتروني

تاريخ استلام المقال: 24 فيفري 2017 تاريخ القبول النهائي: 16 مارس 2017

الأستاذ ذبيح هشام

الدكتور عبد الرؤوف دبابش

أستاذ متعاقد

أستاذ محاضر "أ"

المركز الجامعي بريكا

جامعة محمد خيضر - بسكرة

hichamdebih@gmail.com

المخلص:

أحدث التقدم العلمي الهائل في مجال تقنيات المعلومات، وتدفعها في العقود الثلاثة الأخيرة ثورة إلكترونية تطبق الآن في جميع مناحي الحياة، وأضحى من الصعوبة بمكان الاستغناء عن خدماتها اللامحدودة، مما تم استحداث وسائل عديدة للدفع الإلكترونية يستعملها المستهلك الإلكتروني، إلا أن هذا الأخير لم يسلم من الاعتداء على وسائله الإلكترونية للدفع، حيث تعرضت للقرصنة والتزوير والسرقة، وتغيير الصور التي عليها، وتعديل بيانات بطاقات الدفع الإلكتروني وغيرها ومن الاعتداءات الغير مشروعة المرتكبة في حق المستهلك الإلكتروني، مما دفع إلى جميع الفاعلين في المجال الاقتصادي والمعلوماتي والقانوني إلى توفير الحماية الكافية لدفع تلك الاعتداءات. فمن خلال هذه الورقة البحثية نحاول تسليط الضوء على نوعين من الحماية، أولها الحماية التقنية لوسائل الدفع الإلكترونية التي يستعملها المستهلك، وذلك ببيان إلى أين توصل المجال التكنولوجي إلى تطوير وسائل الدفع الإلكترونية لحمايتها أكثر من الاعتداءات التي تعترضها، وبيان كيف يمكن للمستهلك الإلكتروني استغلالها، ثم بيان الحماية الثانية للمستهلك الإلكتروني، وهي الحماية القانونية، وذلك ببيان المسؤولية المدنية والجزائية المترتبة عن الاستعمال الغير المشروع لوسائل الدفع الإلكتروني، وتوضيح ما مدى كفايتها لتحقيق الحماية المنشودة للمستهلك الإلكتروني.

فيكون الإشكال الذي يتمحور حوله موضوع المدخلة: ما هي الحماية التقنية والقانونية لوسائل الدفع الإلكتروني في ظل التشريع الجزائري وتكنولوجيا الاتصالات الرقمية؟ وهل هي كفيلا بتحقيق الأمان في المعاملات المالية للمستهلك الإلكتروني؟ وللإجابة على الاشكالية تتبع الخطة التالية: المبحث الأول: الحماية التقنية لوسائل الدفع الإلكتروني، أما المبحث الثاني: الحماية القانونية لوسائل الدفع الإلكتروني.

الكلمات المفتاحية: وسائل الدفع المالية - حماية تقنية وقانونية - مستهلك الكرونوي.

Résumé

Les derniers progrès scientifiques considérables dans le domaine des techniques de l'information, et la circulation des trois dernières décennies une révolution Électronique appliquée dans tous les domaines de la vie vallée ,difficile de se passer des services illimité, ce qui a été mise au point de nombreux moyens de paiement électroniques utilisés par les consommateurs en ligne, mais que ce dernier n'a pas remis de l'agression contre ses propres outils électroniques de paiement, où ont été piraterie depuis la falsification, de vol et de changer l'image qui, de modifier les données de cartes de paiement électronique et autres et les attaques contre des tiers illicites commis dans le droit des consommateurs électronique, ce qui a amené à tous les acteurs dans le domaine



économique et informatique, juridique et à assurer une protection suffisante pour le paiement de ces attaques.

Grâce à ce document de recherche nous tentons de mettre en relief les deux types de protection, tout d'abord de protection technique des moyens de paiement électroniques utilisés par les consommateurs, en fait une déclaration où le domaine technologique au développement de moyens de paiement électronique pour les protéger plus d'attaques qu'ils rencontrent, et indiquer comment les consommateurs en ligne de l'exploitation, et la Déclaration de protection deuxième consommateur électronique, protection juridique, dans une déclaration de responsabilité civile pénaux découlant de l'utilisation d'autrui Projet de moyens de paiement électronique et de préciser que l'adéquation de la protection nécessaire aux consommateurs électronique
S'effectue les formes axée autour de la question intervention:Quelle est la protection technique, juridique et des moyens de paiement électroniques dans la législation algérienne et de techniques de communication numériques? Sont-elles capables d'assurer la sécurité des transactions financières consommateur électronique?

Pour répondre à la problématique de suivre le plan suivant:PartI: protection technique des moyens de paiement électroniques, Part II: protection juridique des moyens de paiement électroniques.

Mots clés: moyens de paiement financières protection techniques et juridiques consommateur électronique

مقدمة:

نتيجة للتطور السريع في المعاملات التجارية، واتساع الحياض الاقتصادية، وكثرة المعاملات المالية بين الأفراد والتزاماتهم، وما صاحب ذلك من تقدم في وسائل التكنولوجيا الحديثة التي كان لها دور أساسي في تطور أساليب المعاملات البنكية.

ويعتبر العمل المصرفي الإلكتروني من الأمور التي أفرزها التطور التكنولوجي الهائل في مجال الاتصالات، حيث تم استحداث وسائل دفع جديدة للاثمان والوفاء فاقت في أهميتها الأوراق التجارية، تكون ملائمة لطبيعة ومتطلبات التجارة الإلكترونية، وأصبح بإمكان العميل الاستفادة من الخدمات المصرفية عن طريق الاتصال الهاتفي والإلكتروني.

لكن ورغم المزايا العديدة التي وفرتها المعاملات المصرفية الإلكترونية، إلا أنها في نفس الوقت محفوفة بالعديد من المخاطر، كون هناك ارتباط وثيق بين العمليات الإلكترونية وأمن المعلومات التي قد تؤدي الى العبث في أرصدة العملاء ذاتها، أو إجراء عمليات التحويل الدفع الإلكتروني مبتكره من خلال حسابات العملاء، حيث شهدت حالات كثيرة من الاعتداءات عن طريق القرصنة، والسرقة، والتزوير على الخط التي عرفت صدى كبير خاصة الاعتداء على أرقام بطاقات الدفع البنكية، وتغيير بيانات الرسائل الإلكترونية فأصبحت هذه التقنية شر لا بد منه في ظل حتمية الاندماج في العولمة المفروضة.

ونظرا لذلك كان من الضروري مواجهة هذه السلبيات بتوفير الوسائل القانونية والتقنية لضمان السير الحسن لمعاملات التجارة الإلكترونية ومجال المعلوماتية، من أجل تطويرها خاصة ما يتعلق بالدفع الإلكتروني من خلال خلق الجو الملائم لإتمامها والاجتهاد مع مختلف المؤسسات من بنوك وجامعات ومختصين في الاعلام الآلي والبرمجيات قصد التطوير.

_____ د. عبد الرؤوف دبابش - جامعة بسكرة/ أ.ذبيح هشام - المركز الجامعي بركة (الجزائر)

وتبرز أهمية الدراسة من خلال هذه الورقة البحثية بعرض مختلف الجوانب الجوهرية القانونية والتقنية للدفع الإلكتروني من حيث تنظيم التعامل به، وتبسيط الضوء على الحماية من المخاطر التي يتعرض لها، ثم بيان كيفية التصدي لها من قبل المستهلك الإلكتروني، قصد تحقيق الضمان والأمان والسرعة التي تستوجبها الأعمال التجارية للأهمية الكبيرة التي يلعبها في التجارة الإلكترونية.

ونتيجة لذلك يكون الإشكال الذي يتمحور حوله موضوع المداخلة :

ما هي الحماية التقنية والقانونية لوسائل الدفع الإلكتروني في ظل التشريع الجزائري وتكنولوجيا الاتصالات الرقمية؟ وهل هي كفيلة بتحقيق الأمان في المعاملات المالية للمستهلك الإلكتروني؟

ولإجابة على الاشكالية نتبع الخطة التالية :

المبحث الأول: الحماية التقنية لوسائل الدفع الإلكتروني.

المبحث الثاني: الحماية القانونية لوسائل الدفع الإلكتروني.

المبحث الأول: الحماية التقنية لوسائل الدفع الإلكتروني

نتيجة للتطور الحاصل في المجال الإلكتروني تم استحداث وسائل عديدة يستخدمها المتعاملون قصد الوفاء بما اقتنوا من سلع وخدمات، وهي وسائل الدفع الإلكتروني التي يعتبر استعمالها ذا بعد داخلي وفي نفس الوقت عالمي، حيث تسعى الكثير من المؤسسات إلى تحديث تقنياتها ووضع برامج خاصة بهدف وضع التقنية حيز التنفيذ، إلا أن وسائل الدفع الإلكتروني لم تسلم من الغش والسرقة مما أُلزم إيجاد تقنيات جديدة لحماية المستهلك الإلكتروني من ذلك، وهذا ما سيم عرضه من خلال ما هو موضح أدناه.

المطلب الأول: تعريف الحماية التقنية للدفع الإلكتروني.

قبل اللجوء إلى معرفة الحماية التقنية، لابد من معرفة ما المقصود بالدفع الإلكتروني، وكيف يتعرض المستهلك الإلكتروني إلى الغش والتدليس، من خلال استخدام بطاقات الدفع الإلكتروني.

أولاً: تعريف الدفع الإلكتروني: المصطلح مكون من شقين، الأول يعالج تقنية الدفع،

والثاني يعالج مصطلح الكتروني:

وسائل الدفع ما بين الحماية التقنية والقانونية للمستهلك الإلكتروني

أ- المقصود بمصطلح الإلكتروني: تقنية كهروبايئة، رقمية مغناطيسية، بصرية، الكترومغناطيسية أو أي شكل آخر من أشكال التكنولوجيا، يضم إمكانات مماثلة لتلك التقنيات، أو بمعنى آخر استخدام لكل قطاعات الاتصال عن بعد¹.

ب- المقصود من تقنية الدفع الإلكتروني: مجموعة الخطوات التي تبدأ بأمر التحويل الصادر عن المستفيد بهدف الدفع للمستفيد من الأمر، ويتم ذلك شفويا، الكترونيا، كتابيا، ويشمل ذلك أي أمر صادر عن بنك الأمر، أو البنك الوسيط يهدف إلى تنفيذ أمر الأمر بالتحويل، ويتم النقل بقبول بنك المستفيد دفع قيمة الحوالة لمصلحة المستفيد المبين في الأمر.

أو هو عقد بين الأمر بالتحويل المصرفي والبنك مصدر الحوالة، يلتزم بموجبه أن يدفع بنفسه أو بواسطة غيره مبلغا من النقود يعادل قيمة الحوالة إلى المستفيد مقابل عمولة متفق عليها².

ثانيا: تعريف الحماية التقنية للدفع الإلكتروني: أنها حماية جميع أنواع المعلومات ومصادر الادوات التي يتعامل معها، من غرفة تشغيل الأجهزة، ووسائط التخزين والأفراد والسرقة والتزوير والتلف والضياع والاختراق³.

كما يمكن تعريف أمن المعلومات بأنه " حماية وتأمين كافة المواد المستخدمة في معالجة المعلومات، حيث يتم تأمين المنشأ نفسها والأفراد العاملين فيها وأجهزة الحاسبات المستخدمين فيها ووسائط المعلومات التي تحتوي على بيانات المنشأ، ويتم ذلك عن طريق إتباع إجراءات ووسائل حماية عديدة تضمن في النهاية سلامة المعلومات وهي الكنز الثمين الذي يجب على المنشأ المحافظة عليه⁴.

ثالثا: أهمية الحماية التقنية للمعلومات.

إن حماية الدفع الإلكتروني والبيانات عامة شيء بالغ الأهمية للبنوك ويترجم ذلك من خلال المبالغ المالية المستثمرة في هذا المجال من جهة، كما تعتبر الأكثر عرضة للقرصنة، ويشكل الاعتماد على الحسابات البنكية جريمة التحويل الإلكتروني غير المشروع للأموال.

¹ - جمال زكي الجريدي، البيع الإلكتروني للسلع المقلدة عبر شبكة الانترنت، دراسة فقهية مقارنة، دار الفكر الجامعي، مصر 2008، ص 10.

² - محمد عمر ذوابة، عقد التحويل المصرفي الإلكتروني، دار الثقافة للنشر والتوزيع، مصر، 2006، ص 23.

³ - محمد دباس حميد، حماية أنظمة المعلومات، دار الحامد، الأردن، 2007، ص 34.

⁴ - حسن طاهر داود، الحاسب وأمن المعلومات، معهد الإدارة العامة، مكتبة الملك فهد الوطنية، الرياض، ص 23.

_____ د. عبد الرؤوف دبابش - جامعة بسكرة/ أ.ذبيح هشام - المركز الجامعي بريكا (الجزائر)

وعلى سبيل المثال فإن بنك BNP Paribas قام بتسخير 2.8 مليار أورو، فالاستثمارات في أمن المعلوماتية في تطور مستمر، وهذا تماشيا مع طبيعة المخاطر التي تهدد الأنظمة وبالتالي ضرورة جعلها آمنة واستقلالها لرفع من دخل البنك.

رابعا: طبيعة أمن المعلومات والبيانات.

الاستعمال الهائل لشبكة الانترنت، أدى إلى إقحام كل المتعاملين في التجار الإلكترونية عامة وفي الدفع الإلكتروني والتحويل الإلكتروني للأموال خاصة إلى اهتمام الجميع بضرورة حماية هذه المعاملات.

أ- من حيث المعنيين بتوفير أمن المعلومات: أهمية قضية الأمن ازدادت في الآونة الأخيرة فأصبحت مشكلة تبحث عن حل، وأصبحت هذه القضية تهم رجال الأعمال والمتعاملين الاقتصاديين وكل من لديه أنظمة ومعلومات، وأصبحت تهم الاستفادة العادي وتهم الشركات التي تقدم خدمات معلومات، وتهم مصممي النظم والتطبيقات، وكذلك الشركات المطورة للأجهزة والبرمجيات، بل هي تهم في الوقت نفسه رجال القانون والتشريع ورجال الأمن، وتهم متخصصي الاتصالات وتهم المدرسين والطلاب.

كما تهم مسئولو الرقابة، سواء الرقابة المالية والرقابة الادارية، وعلى رأسهم هؤلاء جميعا يأتي مسؤولو أمن المعلومات كمهتمين رئيسيين بهذه القضية¹.

ب- من حيث صناعة أمن المعلومات: مشاكل أمن المعلومات تكمن على مستوى المستهلك أي المشتري أو الزبون، على مستوى العنوان الإلكتروني للمؤسسة التجارية تتعامل عبر الأنترنت²، فتأمين المعلومات سمح بضمان من الناحية التكنولوجية المسار الجيد والصحيح للمعاملة التجارية وذلك بالضمان لأنظمة الحواسيب وتأمين تحويل البيانات ما بينها وذلك بالقدرة على:

- القدرة على الاستعمال (توفير هذه الخدمة، الموارد والبرامج اللائقة).

- عدم السماح بالدخول للمعطيات والموارد الرقمية، سوى للأشخاص والبرامج ذات الاختصاص لضمان (السرية، صحة البيانات والمعطيات وكذلك الخدمات).

- التأكيد وتبيان أن المعاملة قد حدثت فعلا (سيرورة المعاملة، دلائل وعدم الرجوع).

- تطبيق المعاملة وجعل الخدمات المرجوة في أوضاع جيدة والاستعمال اللائق (استمرارية الخدمات، أمن الاستعمالات وفعالية البرامج)³.

¹ - المرجع نفسه، ص 26.

² - Solange Ghernaoui-Hélie·Sécurité·Internet·strategie et technologie et technologie· Edition Dunod· Paris· 2000· p229.

³ - Solange Ghernaoui-Hélie·Sécurité·Internet·strategie et technologie et technologie· ip.id· p228.

وسائل الدفع ما بين الحماية التقنية والقانونية للمستهلك الإلكتروني

كما يمكن تطبيق مجموعة من الاجراءات للحد من مخاطر الاعتداءات المعلوماتية، وخطر التزوير وذلك من خلال ما يلي:

- اختراع نظام أمن (Un label de sécurité) وذلك بتوحيد الأنظمة الموجودة.
- المراقبة والتأكيد الشديدين لهوية الأطراف المتدخلة في العملية، ووضع نظام فعال للتأكد من هذه الأنظمة.
- إدماج أمن المحتويات الرقمية في السياسة الأمنية تماشياً مع التطورات والمستجدات التكنولوجية.
- تقوية حماية المستهلكين، بتحسيس المستعملين بالأخطار التي يمكن أن يواجهها مسار نقل المعلومات ما بين مراكز المعلومات والبنوك،
- التأكد من الدفع والطلب بالوسائل الخارجية عن شبكة الإنترنت كالهاتف مثلاً.
- استعمال اجراءات وتقنيات أمنية إضافية.

المطلب الثاني: الميكانيزمات التقنية لعملية الدفع الإلكتروني.

لقد دفع الطابع غير المادي للدفع الإلكتروني إلى ضرورة إيجاد وسائل وتقنيات وضعت تحت تصرف المتعاملين بها كي يضمن أكبر قدر ممكن من الثقة والاطمئنان من خلال انجاح استعمالها، وذلك بانتشارها في كافة المعاملات المالية والتجارية، ومن تلك التقنيات مثل التوقيع الإلكتروني والرقمي، وتشفير المعلومات والبيانات المرسله على الخط، وتقنيات أخرى يتم توضيحها أدناه.

أولاً: الرقم السري والكلمات السرية: تعتبر الحماية بواسطة الرقم السري الإجراء المؤمن الأكثر استعمالاً في المجال الرقمي في عصرنا الحالي، واجراءات فتح النافذة واستعمال الرقم السري يسمح لصاحب البرامج التأكد من هوية المستعمل الذي يحاول الدخول إلى العنوان الإلكتروني أو جزء منه، وذلك عند محاولته الدخول لنافذة مؤمنة، يجب استعماله لرقم السري لتأمين معاملاته، وعند تقديمه للرقم السري الصحيح يمكنه الدخول لما يريده من المعطيات والبيانات السرية والشخصية¹.

¹ -Jeffrey F Rayport، Bernard J.Jaurorski،commerce électronique، Edition cheneliere،McGram-Hill،Montréal-toronto، 2003، p56.

ثانيا: التوقيع الالكتروني:

أ- تعريفه:

التوقيع الالكتروني عبارة عن ملف رقمي صغير مكون من بعض الحروف والأرقام والرموز الالكترونية تصدر عن إحدى الجهات المتخصصة والمعترف بها حكوميا ودوليا ويطلق عليها اسم الشهادة الرقمية.

ويخزن في هذا الملف جميع معلومات الشخص وتاريخ ورقم الشهادة ومصدرها وعادة يسلم مع هذه الشهادة مفتاحان أحدهما عام والآخر خاص، أما المفتاح العام فهو الذي ينشر في الدليل لكل الناس والمفتاح الخاص هو توقيعك الالكتروني وتقوم الهيئات بإصدار تلك الشهادات الرقمية والتي تكون مقابل رسوم معينة.

وبذلك فالتوقيع الالكتروني هو طريقة اتصال مشفرة رقميا تعمل على توثيق المعاملات بشتى أنواعها والتي تتم عبر صفحة الانترنت¹.

ب- أنواع التوقيعات الالكترونية:

1- التوقيع الرقمي: وهنا يتم تزويد الوثيقة الالكترونية بتوقيع رقمي مشفر تقوم بتشخيص المستخدم "الموقع" الذي قام بالتوقيع ووقت التوقيع ومعلومات الشخص نفسه وهو عادة مميزا لأصحاب التوقيع.

2- التوقيع البيومترى: يقوم الموقع هنا باستخدام قلم إلكتروني، يتم توصيله بجهاز الكمبيوتر، ويبدأ الشخص بالتوقيع باستخدام القلم مما يسجل نمط حركات يد الشخص وأصابعه، ولكل منا نمط مختلف عن الآخر، حيث يتم تحديد هذه السمة، وهنا تقودنا أيضا إلى البصمة الالكترونية التي تعمل بنفس التقنية.

ج- الهدف من التوقيع الالكتروني: يندرج الهدف تحت مضمون الأمن والسلامة الرقميين وعند ثبوت صحتها فإنها بالطبع تحقق جميع الجوانب العملية والأهداف المرجوة منها ولعدد أهداف قانونية بحة تبعد المتطفلين عن التلصص وسرقة البيانات².

د- التوقيع الالكتروني في القانون الجزائري: لقد ذكر التشريع الجزائري مسألة التوقيع الالكتروني واعترف به في القانون المدني³ في المادة 323 مكرر 1 بنصها (يعتبر الإثبات

1 - حايث أمال، استقلال خدمة الأتترنت، مذكرة للنيل درجة الماجستير في الحقوق، فرع قانون الأعمال، جامعة مولود معمري، تيزي وزو، 2004، ص 86.

2 - أسامة الكسواني، التوقيع الالكتروني، المجلة الالكترونية، مقال منشور على الموقع الالكتروني: <http://news.maktoub.com/article> ص3.

3 - الأمر 58/75 المؤرخ في 20 رمضان 1395 الموافق لـ 26 سبتمبر 1975، المتضمن: القانون المدني، المعدل والمتمم بالقانون 05/07 المؤرخ في 13 مايو 2007. (الجمهورية الجزائرية، الجريدة الرسمية، عدد 18، 2007).

وسائل الدفع ما بين الحماية التقنية والقانونية للمستهلك الإلكتروني _____
بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق..)، وما يلاحظ أن الدولة
الجزائري بدأت تطبق مسألة التوقيع الإلكتروني في الكثير من الوثائق الإدارية، كالوثائق
البيوميتريّة للهوية مثل جواز السفر وبطاقة التعريف الوطنية، وهذا يعد من قبل الاعتراف
بالتوقيع الإلكتروني وتوسيع مجالات استعماله.

ثالثا: تشفير البيانات كتقنية لتأمين الدفع الإلكتروني:

أ- تعريف التشفير (Encrypt):

يطلق عليه لفظ التعمية، للتعبير عن الرسالة المشفرة بحيث لو تم اعتراض الرسالة فلا
ينكشف مضمونها، وهو وسيلة للحفاظ على أمن المعلومات من نية غير آمنة.

فالتشفير تعتبر تقنية تكنولوجية تستعمل خورزميات رياضية معقدة لتشفير ونزع
تشفير البيانات وهذا بهدف ضمان السرية التي تستلزمها المعلومات بقصد تأمين المعلومات ما بين
الزبون على الخط والتاجر أو البنك بقصد أن تنحصر قراءتها والإطلاع عليها على المعنيين
الشرعيين لهذه العملية¹.

ب- آلية استخدام التشفير:

يستلزم استخدام تشفير المعلومات تركيب برامج مخصصة لذلك على حاسوب كل من
المرسل ومتلقي المعلومة أو البيانات، فبعد كتابة الرقم السري للبطاقة أو رقم الحساب، يستعمل
البرنامج المخصص للتشفير لتشفير هذه الأرقام قبل بعثها إلى التاجر أو البنك، فيتلقى التاجر
أو البنك هذه الرسالة مشفرة فيستعمل بدوره البرنامج المخصص لفك التشفير ليتمكن من
قراءتها، وإذا تمكن شخص بطريقة أو بأخرى الحصول على نسخة من الرسالة فلا يمكنها
قراءتها لأنها مشفرة.

ج- أهمية التشفير لتأمين البيانات:

عن طريق هذه التقنية يمكننا التغلب وتجاوز الكثير من المخاطر، فبواسطتها نتجنب:

- الاطلاع على المعلومات المحظورة (السرية) والشخصية.
- محاولة تعديل البيانات المنقولة بالشبكة.
- إعادة توجيه البيانات إلى جهة أخرى.
- تغيير محتويات الرسائل المتبادلة.
- تغيير كلمات السر الخاصة بالمستفيدين.
- انتحال شخصية المستخدم الحقيقي.

¹ -Jeffrey F Rayport، Bernard J.Jaurorski، commerce électronique، op.cit، p57.

_____ د. عبد الرؤوف دبابش - جامعة بسكرة/ أ.ذبيح هشام - المركز الجامعي بركة (الجزائر) - تعديل الحسابات المخزنة على الحسابات نفسها¹.

المطلب الثالث: نماذج من برامج تأمين البيانات الالكترونية.

هناك العديد من برامج أمن مراسلات التجارة الالكترونية وذلك بهدف ضمان الثقة في هذه المعاملات، مما يساعد على تطويرها وترقيتها، ويتم توضيحها أدناه.
أولا: بروتوكول الحركات المالية الآمنة:

يعتبر من أهم بروتوكولات أمن المعلومات الالكترونية لتحقيق غاية ضمان الحفاظ على أمن البيانات، أثناء إجراء الحركات المالية عبر شبكة مفتوحة مثل الأنترنت، يستخدم هذا البروتوكول برمجيات تدعى برمجيات المحفظة الالكترونية.

وتحتوي هذه الأخيرة على رقم حامل البطاقة والشهادة الرقمية التابعة له أما التاجر فتكون له شهادة رقمية صادرة عن إحدى البنوك المعتمدة، ويستخدم كل من حامل البطاقة والتاجر الشهادة الرقمية التابعة له مما يتيح لكل منهما التحقق من هوية الآخر عند إجراء الحركات المالية عبر الأنترنت.

ولا يمكن للتاجر مشاهد رقم البطاقة الائتمانية أثناء استعمال بروتوكول الحركات الآمنة، حيث ترسل الصيغة المشفرة لهذا الرقم الى مصدر هذه البطاقة للموافقة على إجراء الحركة المالية مع التاجر، وتضمن هذه الطريقة عدم عرض الرقم، كما تمنع أي تعديل مرخص به أثناء إرسال البيانات².

ثانيا: نظم أمن الحسابات المركزية:

بالنسبة لعالم الحسابات المركزية الكبيرة لا يوجد الكثير من نظم الأمن في الأسواق، وربما السبب هو سيطر بعض الشركات الكبرى على سوق الحسابات المركزية، وتتميز هذه السوق بضخامة الانتاج، حيث يجب أن يكون نظم الأمن شاملة ومتناغمة مع نظام التشغيل الرئيسي مع العديد من نظم التشغيل المساعدة، ولذلك تحجم شركات نظم أمن المعلومات الصغيرة عن الدخول إلى هذه الأسواق وتنفرد به شركات مثل (IBM) لذلك على رأس نظم أمن الحسابات المركزية الشهيرة نظامان هما: نظام "راكف" (Ressource Access Control Facility)، ونظام (Access control Facility)³.

¹ - حسن طاهر داود، المرجع السابق، ص 178.

² - إبراهيم بختي، التجارة الالكترونية، ديوان المطبوعات الجامعية، الجزائر، 2005، ص 79.

³ - محمد دباس حميد، حماية أنظمة المعلومات، المرجع السابق، ص 105.

ثالثا: نظم أمن الحسابات الشخصية:

ومن بينها برنامج "بي سي سيف" الذي انتجته شركة إنيجما لوجيك فهو برنامج يستخدم كلمة مرور لمرة واحدة فقط لتنظيم استخدام الحاسب، فيقدم بذلك أسلوبا للتحكم في استخدام البيانات يطلق عليه "التحكم المحمول"، إذ يمكن استخدام البيانات حيث يحدثون كلمة المرور التي تستخدم مرة واحدة، ولا يشترط أن يكون ذلك من خلال نظام التشغيل الذي تم من خلاله تشفير البيانات بل من خلال أي نظام تشفير آخر، وهذا البرنامج يتطلب وسائل خاصة يتيح استخدام كلمة المرور التي تستخدم لمرة واحدة وهذا لعتاد محمول هو الآخر

رابعا: برنامج ديسك ووتشر:

فهو واحد من المجموعة التي صممت لحماية البيانات، ولضمان عدم محوها عن طريق خطأ غير مقصود من جانب المستخدم¹.

خامسا: تقنية الحماية 3DS:

هو نظام يوفر أعلى مستويات الحماية لعمليات الدفع عبر الأنترنت، فيساهم في تخفيض نسبة الأخطار أو المشاكل التي تحدث خلال عملية الشراء عبر الأنترنت، من خلال من خلال تمكين المصاريف المتخصصة في إصدار البطاقات والتحقق من هوية الشخص الذي قام بإجراء المعاملة التجارية الإلكترونية وتوفير تقنية "3DS" حماية إضافية حيث تتم العمليات الإلكترونية أمام الشخص مباشرة.

كما يعتمد على نظام التشفير (SSL) ومأخذ Merchant server لتمرير المعلومات والتأكد من هوية حامل البطاقة خلال عمليات الشراء التي تتم على الخط، ويجمع هذا النظام بين السهولة ومرونة التطبيق، ويوفر الانتقال الآمن لتفاصيل الحساب وتخفيض نسبة الأخطاء².

المبحث الثاني: الحماية القانونية لوسائل الدفع الإلكتروني

نظرا لتعدد استخدام وسائل الدفع الإلكتروني في المجال التجاري والمعاملاتي من قبل المستهلكين، باستعمال بطاقات الدفع الإلكتروني، أدى ذلك في الكثير من الأحيان التعدي عن تلك البطاقات من قبل الجناة عن طريق القرصنة، كتزوير تلك البطاقات كليا بإنشاء بطاقات مماثلة لها، أو جزئيا بتعديل بعض البيانات فيها، أو التعدي عليها بالسرقة وال نصب والاحتيال، مما دفع بالمشروع الجزائري إلى توفير القدر الكافي من الحماية القانونية للمستهلك الإلكتروني،

¹ - المرجع نفسه، ص 106.

² - steven j. Murdoch et Ross Anderson، vérifié par visa et master Card secure cod، étude du laboratoire informatique، univesité de Cambridge، royaume uni، in: <http://www.cl.cam.uk/users/p2>.

_____ د. عبد الرؤوف دبابش - جامعة بسكرة/ أ.ذبيح هشام - المركز الجامعي بريكّة (الجزائر)
وذلك من خلال تحميل المسؤولية المدنية والجزائية لكل مرتكب لجريمة معلوماتية تتعلق بالدفع الإلكتروني، أو حتى سبب الإهمال والخطأ يرتب على ذلك مسؤولية، يستفيد منها المستهلك الإلكتروني المتضرر من الفعل المرتكب.

المطلب الأول: المسؤولية المدنية الناشئة عن الاستخدام غير المشروع لبطاقات الدفع الإلكتروني.

أولاً: المسؤولية المدنية لمصدر البطاقة وحاملها.

1- المسؤولية المدنية لمصدر البطاقة :

تلتزم الهيئة المصدرة لبطاقات الدفع الإلكتروني، بسداد المبالغ والفواتير المرسلّة لها من التاجر، وذلك في مواجهة الحامل والتاجر طالما أنهما قاما بالالتزامات العقدية اتجاههما، فإذا أخلت الجهة المصدرة بهذا الالتزام وترتب على ذلك ضرر للحامل، كتفويت صفقة تجارية كان يعتمد في إبرامها على رصيده، أو توقف التاجر عن سداد ديونه مما أدى إلى قيام الدائن بالهجر عليه وإساءت سمعته التجارية أو غير ذلك من الأضرار حينها تنعقد المسؤولية المدنية للجهة المصدرة للبطاقة على أساس تعاقدية، طالما أن كل من الحامل للبطاقة والتاجر قاما بتنفيذ شروطهما العقدية معها¹.

كما تنعقد المسؤولية المدنية للجهة المصدرة متى قامت بوفاء الفواتير التي تصل إليها بعد إعلانها بواقعة السرقة أو الضياع، إذ أن من واجبها التزام الحيطة والحذر من الاستعمال الغير المشروع لبطاقة الدفع الإلكتروني، وذلك من خلال إخضاع هذه الفواتير لإجراءات مشددة من حيث الرقابة على صحة التوقيع الذي تحمله هذه الفواتير، فقد يكون التوقيع مزوراً، حتى وإن كان مثبتاً على الفاتورة تاريخ مسبق بقيمة النفقات دون تغيير بيانات الكشوف الواردة للتاجر².

أو قد يحدث أن الحامل يقوم بالتبليغ عن فقدان بطاقته أو سرقتها، لكن الجهة المصدرة لا تسارع إلى تعميم البطاقة المسروقة على الجار والمحلات مما يشكل إخلالاً بالالتزام جوهرية لها، إذا ما تحقق يكون سبباً موجباً لمساءلتها، لذلك يقع عليها عدم قبول أية معاملة تتم ببطاقة مسروقة أو ضائعة، إضافة إلى الإسراع بتعميم أرقام تلك البطاقات مع تشديد حرصها على عدم سداد أي مبالغ تتم بواسطة استخدام بطاقة مسروقة، وإذا قامت الجهة المصدرة بخلاف

¹ - كميّة طالب البغدادي، الاستخدام الغير المشروع لبطاقة الائتمان، دار الثقافة، الأردن، 2008، ص 229.

² - حوالمف عبد الصمد، النظام القانوني لوسائل الدفع الإلكتروني، أطروحة مقدمة لنيل شهادة الدكتوراه، جامعة أبو بكر بلقايد، تلمسان، 2015، ص 512.

وسائل الدفع ما بين الحماية التقنية والقانونية للمستهلك الإلكتروني _____
ذلك، فإنها تكون المسؤولة وحدها عن المبالغ المدفوعة بهذه الطريقة وليس لها مطالبة الجامل بتلك المبالغ¹.

كما تتعدّد المسؤولية المدنية في حالة الوفاء بقيمة العمليات التي تمت بعد إعلامها بواقعة وفاة حامل البطاقة، لأنه معروف أن عقد حامل البطاقة مع الجهة المصدرة قائم على الاعتبار الشخصي، وعليه فإن العمل ببطاقات الدفع الإلكتروني ينتهي أوتوماتيكياً وتلقائياً فور وفاة الجامل².

وتتعدّد مسؤولية المصدر في حدود المبالغ التي يقوم بالوفاء بها، والتعويض عن الأضرار التي تصيب الورثة من جراء هذا الوفاء، وذلك على أساس المسؤولية التقصيرية التي نص عليها القانون المدني الجزائري في المادة 124 (كل من تسبب بخطئه ضرراً للغير ألزم من كان سبباً في حدوثه بالتعويض)، وهذا كان نتيجة لإرتكاب الجهة المصدرة الخطأ في حقهم ما يؤدي إلى إنقاص حقوقهم في التركة، ولأن الورثة ليسوا أطرافاً في العقد بل يكفي أن يثبتوا عنصر الضرر والعلاقة السببية بين فعل الجهة المصدرة حتى ولو لم تقم هذه الأخير بأي خطأ.

2- المسؤولية المدنية لحامل البطاقة:

يلتزم حامل بطاقة الدفع الإلكتروني في حدود مبالغ السقف الائتماني الممنوح له من المصدر، فإذا تجاوز هذا المبلغ كان مسؤولاً مدنياً بمقدار الزيادة في مواجهة مصدر البطاقة في حالة وجود اتفاق بضمان الوفاء دون تحديد الحد الأقصى لهذا الضمان، أما إذا كان مصدر البطاقة لا يضمن الوفاء إلا في حدود المبلغ المسموح به تتعدّد مسؤولية الجامل في مواجهة التاجر بموجب عقد البيع المبرم بينهما، هذا إذا التزم الجامل بتنفيذ العقد بحسن نية، أما في حالة تجاوز المبلغ الائتماني مع علمه بذلك، يتوافر في حقه سوء النية أو الخطأ في تنفيذ التزاماته، ومن حق الجهة المصدرة سحب البطاقة من الجامل نظراً لإهداره الثقة بينه وبين المصدر لقيام البطاقة على الاعتبار الشخصي لحاملها.

وتتعدّد مسؤولية صاحب البطاقة كذلك في حالة انتهاء التاريخ المحدد لاستخدامها أو في حالة إلغائها نتيجة فسخ العقد المبرم بينه وبين المصدر، كونه سيكون مخالفاً في هذه الحالة لأحد شروط العقد الذي يلزم الجامل للبطاقة بردها إلى الجهات المصدرة في حالة انتهاء صلاحيتها أو إلغائها، وعدم السماح له باستخدامها، فإذا رفض الجامل رد بطاقة الدفع

¹ - زرقان هشام، النظام القانوني لبطاقات الدفع الإلكتروني، مذكورٌ لنيل شهادة الماستر، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، 2015/2016، ص 43.

² - محمد توفيق سعودي، بطاقات الائتمان والأسس القانونية للعلاقات الناشئة عن استخدامها، دار الأمين، ط: أ، مصر، 2001، ص 108.

د. عبد الرؤوف دبابش - جامعة بسكرة/ أ.ذبيح هشام - المركز الجامعي بريكة (الجزائر)
الإلكتروني إلى المصدر في حالة إلغائها أو انتهاء مدة صلاحيتها، ولم يتم تجديد العقد تلقائياً
من المصدر ولم يطلب الحامل تجديد العقد يكون الحامل قد أخل بتنفيذ التزامه العقدي، ومن
ثمة يعد مرتكباً لخطأ عقدي يرتب عليه انعقاد المسؤولية العقدية في ذمته¹.

ثانياً: المسؤولية المدنية للتاجر والمسؤولية المدنية للغير:

1- المسؤولية المدنية للتاجر:

يرتبط التاجر بكل من الحامل والجهة المصدر بعقد مستقل يفرض عليه التزامات
اتجاه كل منهما، وعليه يمكن القول إن إخلال التاجر بأحد الالتزامات التي يفرضها عليه أي من
العقدين يرتب عليه التزاماً بالتعويض طالما أن هذا الإخلال رتب ضرراً للطرف الآخر وفقاً
لقاعدة المسؤولية العقدية².

وهذه الالتزامات تتمثل في قبوله بالتعامل بالبطاقة، والتحقق من مدة صلاحيتها،
والقيام بمضاهاة التوقيع الصادر من الحامل بالتوقيع الموجود على البطاقة، وغيرها من
الالتزامات التي يترتب على مخالفتها أو الإخلال بها انعقاد مسؤولية التاجر المدنية.

فمثلاً إخلاله بالتزام قبول التعامل بالبطاقة، يفسح المجال أمام الجهة المصدر لها
بفسخ العقد المبرم بينها وبين التاجر، ومطالبته بالتعويض على اعتبار أن قيامه برفض البطاقة
والتعامل بها من شأنه أن يلحق ضرراً بالجهة المصدر لها، يتمثل في امتناع الأشخاص من
الإشتراك بتلك البطاقات، والذي يؤدي إلى إصابة الجهة المصدر بخسارة فادحة للأموال التي
كانت هذه الجهة تحصل عليها من جراء استخدام بطاقات الدفع الإلكترونية، ومثاله العمولة
والفوائد ورسوم الاشتراك والتجديد والإصدار وغيرها من الإيرادات.

أما مسؤولية التاجر في حالة رفض البطاقة اتجاه الحامل، فإنها تقوم على أساس
المسؤولية التقصيرية لا على أساس العقد المبرم بينهما فهذا العقد لا يفرض على التاجر قبول
البطاقة. وبالتالي فإن من حق الحامل الرجوع على التاجر على أساس الضرر الذي أصابه جراء
رفضه، والذي يجعل التاجر مسؤولاً عن تعويض هذا الضرر، وعليه فإن إخلال التاجر بهذا
الالتزام سيؤدي إلى تعرضه للمساءلة المدنية بنوعيتها العقدية والتقصيرية.

كما يقع على عاتق التاجر الامتناع عن قبول أي بطاقة تم إخطاره بضياعها أو سرقتها،
ويعد هذا الإخطار يتحمل التاجر كافة المبالغ التي تعامل عليها منذ إخطاره، وذلك لأنه ملوم
بالإطلاع على قائمة البطاقات المسروقة أو الضائعة أو الملعأة، والتي ترسل إليه ويتم إخطاره

¹ - حوالمف عبد الصمد، المرجع السابق، ص 567.

² - مجد حمدان الجهني، المسؤولية المدنية عن الاستخدام غير المشروع لبطاقات الدفع الإلكتروني، دراسة المسيرة،
الطبعة الأولى، الأردن، 2007، ص 243.

وسائل الدفع ما يبين الحماية التقنية والقانونية للمستهلك الإلكتروني _____
بها من قبل الجهة المصدرة للبطاقة وبصفة دورية، فتتعدد عند إخلاله بهذا الالتزام مسؤوليته
العقدية تجاه الجهة المصدرة، ومسؤوليته التقصيرية تجاه الحامل، جراء الأضرار التي تصيبه
من الاستخدام غير المشروع للبطاقة من قبل الغير أثناء سرقتها أو ضياعها¹.
وعليه فكل اخلال من قبل التاجر بأي من الالتزامات الواردة في عقده من قبل الجهة
المصدرة لبطاقة الدفع الإلكتروني، يعرضه للمساءلة من قبلها مدنيا على أساس تعاقدية إضافة
إلى مطالبته بتعويض مصدر البطاقة عن أية أضرار تصيبه.

2- المسؤولية المدنية للغير:

نصت المادة 124 من القانون المدني الجزائري على أنه "كل فعل أيا كان يرتكبه الشخص
بخطئه ويسبب ضررا للغير، يلزم من كان سببا في حديثه بالتعويض".
ويتضح من خلال المادة السابقة أن المسؤولية عن العمل الشخصي تشمل الخطأ والضرر
والعلاقة السببية بين الخطأ والضرر الذي يرتكب عنه، وبالتالي يلتزم مرتكبه بالتعويض عن
هذا الضرر.

وبالتالي إذا وقعت بطاقات الدفع الإلكتروني في يد الغير، أي في يد شخص غير حاملها
الشرعي، واستطاع هذا الغير بطريقة أو بأخرى استعمالها وتمكن من الحصول على خدمات
ومشتريات وتحصيل المبلغ من رصيد مالكها الحقيقي، فإنه يعد مسؤولا مدنيا اتجاه الحامل
صاحب هذه البطاقة عن الأضرار التي أصابته، ولكن هذه المسؤولية لا تقوم على أساس
تعاقدية، حيث لا يرتبط الغير بأي رابطة عقدية بحامل البطاقة، ولكنها تقوم على أساس
المسؤولية التقصيرية، فبمجرد إقدام الغير على استخدام البطاقة مع علمه بأنها مملوكة
لشخص آخر يعد خطأ من جانبه، وبالنسبة لركن الضرر فهو متوافر أيضا لأن استعمال الغير
لبطاقة مفقودة أو مسروقة في الوفاء أو في السحب يسبب أضرار مادية لحامل البطاقة، الأمر
الذي يبرر مسؤولية الغير عن هذه الأضرار في مواجهة الحامل².

المطلب الثاني: المسؤولية الجزائية الناشئة عن الاستخدام غير المشروع لبطاقات الدفع
الإلكتروني.

نتيجة لاتساع استعمال بطاقات الدفع الإلكتروني في الكثير من القطاعات من قبل
المستهلك الإلكتروني، وظهور الكثير من التجاوزات والتعدي عن البطاقة الإلكترونية، بالإضافة
إلى بروز أشكال جديدة للإجرام، دفع بالمشروع الجزائري إلى تعديل قانون العقوبات، ووضع

¹ - كميث طالب البغدادي، المرجع السابق، ص 237.

² - جميل عبد الباقي الصغير، الحماية الجنائية والمدنية لبطاقة الإنتمان المغنطة، دار النهضة العربية، مصر،
1999، ص 212.

_____ د. عبد الرؤوف دبابش - جامعة بسكرة/ أ.ذبيح هشام - المركز الجامعي بريكا (الجزائر)
عقوبات جزائية في حق الجنأه مرتكبي الجرائم الاللكتروني، هذا كله بهدف توفير حماية
جزائية للأنظمة المعلوماتية وأساليب المعالجة الآلية للمعطيات وذلك لسد الفراغ القانوني في
بعض المجالات.

وكان التعديل بموجب القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004، المعدل والمتمم
للأمر رقم 156/66 المتضمن قانون العقوبات، والذي أفرد القسم السابع مكرر منه تحت عنوان
"المساس بأنظمة المعالجة الآلية للمعطيات" والذي تضمن ثمانية مواد من (المادأه 394 مكرر إلى
المادأه 394 مكرر¹)، وكل جريمة لها عقوبة معينة :

- مسؤولة الغير الجزائرية عن تزوير أو تقيد البطاقة الاللكترونية :

تتعرض البطاقات الاللكترونية كغيرها من المستندات والمحترات إلى التزوير المادي
بمختلف أشكاله وطرقه، سواء كان التزوير جزئيا كالتغيير في أحد بيانات البطاقة، أو كليا وهو
ما يسمى بالاصطناع، من خلال اصطناع نماذج واستخدامها في الوفاء أو السحب بهدف الاستيلاء
على أموال الغير².

لقد نصت المادأه 219 من قانون العقوبات الجزائري "كل من ارتكب تزويرا بإحدى
الطرق المنصوص عليها في المادأه 216 في المحترات التجارية أو الرسمية أو شرع في ذلك يعاقب
بالحبس من سنة إلى خمس سنوات وبغرامة من 500 إلى 20.000 دج"، وعلى ذلك إذا وقع
تغيير في إحدى بيانات البطاقة الاللكترونية، كالتغيير في البيانات الخاصة كالرقم الحساب أو
اسم الحامل أو تاريخ الصلاحية، فإن الأمر ينطوي على تزوير في محرر عربي صادر عن البنوك
والمؤسسات المالية، ومن ثمة انطباق نص المادأه 219 من قانون العقوبات.

حيث نصت المادأه 394 مكرر المضافة بموجب القانون رقم 23/06 المؤرخ في 20 ديسمبر
2006 على: "يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50.000 دج إلى 200.000
دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات
أو يحاول ذلك.

تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة، وإذا ترتب على
الأفعال المذكورة أعلاه تخريب نظام أشغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى
سنتين والغرامة من 50.000 إلى 300.000 دج".

¹ - محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية، 2007، ص 62.

² - بن عميرو أمينة، البطاقات الاللكترونية للدفع والقرض والسحب، مذكرة ثليل شهادة الماجستير، كلية الحقوق،
جامعة قسنطينة، 2004-2005، ص 153.

فمن خلال المادة 394 مكرر قد رتبت عقوبة الحبس من 3 أشهر إلى 1 سنة كل من استعمل بطاقات الدفع عن طريق الغش لغرض الاستلاء على اموال المستهلك الإلكتروني، وقد زاد المشرع من تشديد العقوبة لتصل إلى 3 سنوات، إذا ترتب على ذلك الاستعمال تعديل أو تغيير في المعطيات الإلكترونية لبطاقات الدفع وآلات المعالجة الإلكترونية.

وتضيف المادة 394 مكرر 1 من قانون العقوبات على أنه " يعاقب بالحبس من ستة أشهر إلى ثلاثة سنوات وبغرامة من 500.000 إلى 4.000.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها".

كما نص هذا التعديل على عقوبة مصادره وسائل ارتكاب الجريمة، وإغلاق المواقع التي تكون محلا لها، وإغلاق المحل أو المكان الذي ارتكب فيه الجريمة وفقا لنص المادة 394 مكرر 6. كما يعاقب التعديل على الشروع في جرائم هذا القسم.

وكانت مواجهة الجريمة المعلوماتية إحدى بنود اتفاق يؤسس شراكة بين الاتحاد الأوروبي والجزائر، عقد بتاريخ 22 أبريل 2002، وتضمن ذلك المادة 86 منه¹.

وتماشيا مع متطلبات البنك الإلكتروني من تنظيم وتسخير وسائل خاصة بالتعامل بها، احتضن مركز البحث وتسيير الاعلام التقني التابع لبنك الفلاحة والتنمية الريفية يوما مهنيا حول موضوع البنك الإلكتروني، بحضور مجموعة من رجال الإعلام الآلي ومختصون في الاتصال البنكي².

نظم هذا اليوم تحت إشراف MAGACT بمشاركة المؤسسة الفرنسية المختصة في هذا المجال، ولقد استهل اللقاء بطرح إشكالية إيجاد سياسة تسمح بتطبيق البنك الإلكتروني، ثم في مرحلة ثانية اقتراح القواعد والأسس التي يقوم عليها النظام، فعرض تطبيقي يبرز فعالية هذه التكنولوجيا الجديدة.

وسار في هذا المسار السياسة البنكية الجزائرية من أجل ضمان عمليات الوفاء الإلكتروني، وفي هذا الشأن أصدر بنك الجزائر تنظيم داخلي رقم 07/05 بتاريخ 28 ديسمبر 2005 يتعلق بأن أنظمة الوفاء، فهذا التنظيم يعرف النظام بين بنكي للدفع أو التسوية، وهو عبارة عن إجراءات وطنية أو دولية، تنظم العلاقات بين طرفين على الأقل تتوفر فيهم صفة بنك أو مؤسسة مالية أو مؤسسة منخرطة في غرفة المقاصة.

¹ - المرجع نفسه، ص 63.

² - زرقان هشام، المرجع السابق، ص 180.

خاتمة:

من خلال ما سبق نصل الى النتائج التالية:

- يعتبر التقدم التكنولوجي من العوامل المساعدة في تطوير تقنيات المعلومات والاتصالات بما يكفل انسياب الخدمات المصرفية بكفاءة عالية، وإن حسن استغلال وسائل وأنظمة الدفع والسداد الإلكترونية هي من عوامل عصرة المنظومة المصرفية لمواكبة تحديات العصر (تكنولوجيا، وخدمات)، ومواجهة ضغط منافسة البنوك الأجنبية الموجهة أساسا لجذب الزبائن.

- تعد مشكلة حماية وسائل الدفع الإلكتروني التي يستعملها المستهلك من أخطر المشكلات التي تواجهها الأنظمة الاقتصادية، ومن ثمة يجب التصدي للمشكلة كحماية البطاقة من التلاعب والتزوير والتغيير في أنظمة المعالجة، ويكون ذلك من خلال الحماية التقنية باستعمال وسائل تقنية جديدة لمواكبة التغير الحاصل في الجريمة المعلوماتية، وكذلك استعمال الحماية القانونية من خلال التشريع العقابي لكل جريمة إلكترونية ماسة بالدفع الإلكتروني من خلال مواد قانون العقوبات من المادة 394 مكرر إلى المادة 394 مكرر 7.

- الترسنة القانونية في الجزائر مازالت تحتاج إلى تحيين لتواكب الجرائم الإلكترونية الحديثة.

- إن نطاق تطبيق أحكام المسؤولية المدنية تحدد بحسب وجود العقد الصحيح القائم ما بين مرتكب الاستخدام الغير مشروع والمضروع من عدمه، بحيث تنشأ في الأولى المسؤولية العقدية وفي الحالة الثانية تنشأ المسؤولية التقصيرية.

- ان المسؤولية المدنية لكل من المصدر والتاجر مسؤولية عقدية إذا خالف الالتزامات المفروضة عليهما، سواء العامة المنصوص عليها في العقد، أو الخاصة بالحد من الاستخدام غير المشروع، ويكونا مسؤولين تقصيريا إذا ارتكبا الاستخدام غير المشروع للبطاقة بصفتها من الغير.

- إن الاجراءات المتخذة للحد من الاستخدام غير المشروع لبطاقات الدفع الإلكتروني هي إما إجراءات إدارية أو قضائية أو تقنية تتخذ من قبل المصدر، أو إجراءات وقائية تتخذ من الحامل والمصدر.

- حتى تنتشر وتنجح وسائل وأنظمة الدفع والسداد الإلكترونية وتؤدي دورها بفاعلية في خدمة التجارة الإلكترونية فإنه يجب العمل على التحكم في تقنيات الاتصال وحماية شبكة الانترنت من الاحتيال وضمان سرية جميع العمليات المصرفية، وتأمين أكثر حماية بخلق إطار فني مهني متخصص، وإطار تنظيمي محكم ذو شفافية في العمل المصرفي وإقامة رقابة صارمة ضابطة لهذه التعاملات.

توصيات:

- اصدار قانون خاص ينظم المعاملات الالكترونية، واجراءات حماية الدفع الالكتروني.
- ضرورة قيام المؤسسات المالية والبنوك المصدرة لبطاقات الدفع الالكتروني والشركات التجارية التي تتعامل بها بتدريب العاملين فيها على جميع طرق الاعتداءات التي يستخدمها الجناة، وذلك من خلال عقد دورات تدريبية تشمل جميع العاملين في القطاعات الأمنية.
- العمل على دعم البحث العلمي لتطوير وسائل الدفع الالكتروني بتقنيات جديدة، لتوفير حماية أكثر لمواجهة الجريمة التي تعترض المستهلك الإلكتروني.
- الاستفادة من خبرات الدول المتقدمة في المجال التقني والقانوني لوسائل الدفع، لتحقيق الحماية الأكبر للمستهلك.

قائمة المصادر والمراجع:

الكتب باللغة العربية:

- 1 - إبراهيم بختي، التجارة الإلكترونية، ديوان المطبوعات الجامعية، الجزائر، 2005.
- 2 - جمال زكي الجريدي، البيع الإلكتروني للسلع المقلدة عبر شبكة الانترنت، دراسة فقهية مقارنة، دار الفكر الجامعي، مصر 2008.
- 3 - محمد عمر ذوابة، عقد التحويل المصرفي الإلكتروني، دار الثقافة للنشر والتوزيع، مصر، 2006.
- 4 - محمد دباس حميد، حماية أنظمة المعلومات، دار الحامد، الأردن، 2007.
- 5 - حسن ظاهر داود، الحاسب وأمن المعلومات، معهد الإدارة العامة، مكتبة الملك فهد الوطنية، الرياض.
- 6 - الأمر 58/75 المؤرخ في 20 رمضان 1395 الموافق لـ 26 سبتمبر 1975، المتضمن: القانون المدني، المعدل والمتمم بالقانون 05/07 المؤرخ في 13 مايو 2007. (الجمهورية الجزائرية، الجريدة الرسمية، عدد 18، 2007).
- 7 - كميث طالب البغدادي، الاستخدام الغير المشروع لبطاقة الائتمان، دار الثقافة، الأردن، 2008.
- 8 - محمد توفيق سعودي، بطاقات الائتمان والأسس القانونية للعلاقات الناشئة عن استخدامها، دار الأمين، ط: 1، مصر، 2001.
- 9 - مجد حمدان الجهني، المسؤولية المدنية عن الاستخدام غير المشروع لبطاقات الدفع الإلكتروني، دراسة المسيرة، الطبعة الأولى، الأردن، 2007.
- 10 - جميل عبد الباقي الصغير، الحماية الجنائية والمدنية لبطاقة الائتمان المغنطة، دار النهضة العربية، مصر، 1999.
- 11- محمد خليفة، الحماية الجنائية لعطيات الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية، 2007.

المراجع باللغة الأجنبية:

- 1-Jeffrey F Rayport، Bernard J.Jaurorski،commerce électronique، Edition cheneleire،McGram-Hill،Montréal-toronto، 2003.
- 2- Solange Ghernaoui-Hélie،Sécurité،Internet،strategie et technologie et technologie، Edition Dunod، Paris، 2000.

الرسائل والمذكرات:

- 1- حوافظ عبد الصمد، النظام القانوني لوسائل الدفع الإلكتروني، أطروحة مقدمة لنيل شهادة الدكتوراه، جامعة أبو بكر بلقايد، تلمسان، 2015.

_____ د. عبد الرؤوف دبابش - جامعة بسكرة/ أ.ذبيح هشام - المركز الجامعي بريكّة (الجزائر)

2- حابيت أمال، استغلال خدمة الأترنت، مذكرة نيل درجة الماجستير في الحقوق، فرع قانون الأعمال، جامعة مولود معمري، تيزي وزو، 2004.

3- بن عميرو أمينة، البطاقات الالكترونية للدفع والقرض والسحب، مذكرة نيل شهادة الماجستير، كلية الحقوق، جامعة قسنطينة، 2004-2005.

4- زرقان هشام، النظام القانوني لبطاقات الدفع الالكتروني، مذكرة نيل شهادة الماستر، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، 2015/2016.
المراجع الالكترونية:

1- أسامة الكسواني، التوقيع الالكتروني، المجلة الالكترونية، مقال منشور على الموقع الالكتروني:
<http://news.maktoub.com/article>

2-steven j. Murdoch et Ross Anderson، vérifié par visa et master Card secure cod، étude du laboratoire informatique، univesité de Cambridge، royaume uni، in: <http://www.cl.cam.uk/users>.

