

حماية المستهلك من خلال تأمين وسائل الدفع الإلكتروني Consumer protection through secure electronic payment methods.

الدكتورة: أسماء بعلوج	المنتصر بالله أبو طه
أستاذة محاضرة قسم أ	عضو بمخبر النظام القانوني للعقود
كلية الحقوق والعلوم السياسية	والتصرفات في القانون الخاص
جامعة الجيلالي بونعامة، خميس مليانة	جامعة الجيلالي بونعامة، خميس مليانة
Noui1274@hotmail.fr	a_abutaha@univ-dbkm.dz

الملخص

إن المشرع الجزائري عمل على حماية وسائل الدفع الإلكتروني وتأمينها، وذلك من خلال مجموعة من القوانين، وكان آخرها صدور قانون رقم 05/18 المتعلق بالتجارة الإلكترونية، والذي عزز من هذه الحماية ومن خلال ربط هذه الأخير بنظام تصديق مؤمنا، ومرخصا به وفقا للتشريع المعمول به.

كما خول المشرع الجزائري البنك الجزائر الجهة المكلفة برقابة لضمان استجابتها لمتطلبات التشغيل البيئي وسرية البيانات وسلامتها و أمن تبادلها وحمايتها، وهذا من أجل نشر الثقة لدى جمهور المستهلكين لتشجيع التعامل بالتجارة الإلكترونية، ومواكبة التطور التكنولوجي للمعلومات ورفع مستوى الاقتصاد الوطني والوعي الثقافي في أوساط جمهور المستهلكين المتعاملين عبر المواقع الإلكترونية.

الكلمات المفتاحية: الدفع الإلكتروني؛ تأمين الدفع الإلكتروني؛ الحماية الفنية لوسائل الدفع الإلكتروني؛ الحماية البنكية لوسائل الدفع الإلكتروني؛ حماية القانونية لوسائل الدفع الإلكتروني.

Abstract:

The Algerian legislator has worked to protect and secure the means of electronic payment, through a set of laws, the latest of which is Law No. 18/05 on electronic commerce, which strengthened this protection by linking the latter with a secure certification system, and licensed in accordance with the legislation.

The Algerian legislator also authorized the monitoring body to ensure its responsiveness to the demands of interoperability, data confidentiality, integrity, exchange and protection, in order to spread confidence among the consumer audience, encourage dealing with e-commerce, keep pace with the development of information technology, and raise the level of national economy and cultural awareness among the consumer audience dealing through the website.

Key Words:

Electronic Payment, Secure online Payment, Technical Protection For Electronic Payment Methods ,Bank protection of electronic payment methods, Legal protection of electronic payment methods .

مقدمة

يشكل نظام الدفع الإلكتروني عاملاً أساسياً في الاقتصاد بفعل التطور العلمي والتقني بالنظر لاستخدامه في تسهيل المبادلات والمعاملات المالية والتجارية لتحقيق الأهداف المخطط لها في تنمية الاقتصاد الدولي بصفة عامة والوطني بصفة خاصة.

ورغم اتساع نطاق التجارة والمعاملات المصرفية الإلكترونية عبر الانترنت في مختلف دول العالم، فإن ثمة تحديات تعترض هذه المعاملات – خاصة تلك التي يكون أحد أطرافها المستهلك – وتحد من عنصر الثقة والضمان أثناء تنفيذها، هذا ما دفع العديد من الشركات في مجال تكنولوجيا المعلومات، إلى تطوير النظم الخاصة بالحماية في المواقع التجارية على شبكة الانترنت لتوفير الثقة للمستهلك.¹

فتعدد المخاطر الناتجة عن استخدام شبكة الانترنت، التي يتعرض لها المستهلك منها ما يتعلق بانتحال الشخصيات أو اختراق المواقع والعبث بمحتواها والاستخدام الغير المرخص به وغيرها من المخاطر، وللحماية من تلك المخاطر ومن أجل استقرار المعاملات التجارية الإلكترونية، أصدر المشرع الجزائري ترسانة قانونية تعمل على حماية وتأمين وسائل الدفع الإلكتروني، وكان آخرها صدور قانون التجارة الإلكتروني رقم 50/18، وهذا من أجل مواكبة التطور التكنولوجي المعلومات ومسايرة الاتفاقيات الدولية والإقليمية التي انتهجت نفس السياق في مجال ذات الحماية.

ومن هنا نطرح الإشكالية التالية:

الإشكالية: ما هي الطبيعة القانونية لحماية المستهلك في وسائل الدفع الإلكتروني؟

وللإجابة عن هذه الإشكالية نقسم هذا الموضوع إلى مبحثين، سنتطرق في المبحث الأول إلى تقنيات أمن العمليات الإلكترونية، ثم سنتطرق إلى تأمين الدفع الإلكتروني في المبحث الثاني.

المبحث الأول

تقنيات أمن العمليات الإلكترونية

تعتمد تقنيات أمن العمليات الإلكترونية على تقنيات تعمل على تحديد هوية المتعامل الإلكتروني من جهة، وسلامة تبادل البيانات الإلكترونية من جهة أخرى، وعليه قسمنا هذا المبحث إلى مطلبين، سنتطرق في المطلب الأول تقنيات تحديد الشخصية والوثوق في هوية المتعاقدين، وسنتطرق في المطلب الثاني إلى تقنية أمن المراسلات والمواقع الإلكترونية.²

المطلب الأول

تقنيات تحديد الشخصية والوثوق في هوية المتعاقدين

اشترط المشرع الجزائري لقبول الكتابة المتخذة شكلا إلكترونيا ومنحها الحجية اللازمة في الإثبات أن يكون في الإمكان تحديد هوية الشخص الذي صدرت منه بالأوضاع المقررة في المادة 323 مكرر 1 من القانون المدني التي تنص على أنه: "يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق، بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها".

وأكد المشرع الجزائري على ضرورة التأكد من هوية المتعاملين في البنوك في النظام رقم 11 - 08 المؤرخ في 28 نوفمبر 2011،³ يتعلق بالرقابة الداخلية للبنوك والمؤسسات المالية في المادة 29 التي تنص على: "...السهر على التحديد الدقيق لهوية الأمر بالعملية والمستفيد من التحويلات الإلكترونية، بالإضافة إلى عنوانيهما مهما كانت الوسيلة المستعملة...".

ومما لا شك فيه أن مسألة التأكد من هوية الأطراف لا تشكل أية صعوبة في مجال القواعد العامة في العقود، مثلما هو الحال في التعاقد بالمراسلة، بينما تزيد تلك المسألة تعقيدا إذا ما كان ذلك التعاقد يتم عن بعد من خلال شبكة الانترنت، ويرجع السبب في ذلك إلى الصفة المفتوحة والحرّة والتفاعلية للشبكة، وتعدد المتدخلين في العملية التعاقدية،⁴ سواء كانوا مزودي خدمات الانترنت أو مقدمي خدمات التصديق الإلكتروني.

ويقصد بالوثوق في هوية المتعاقدين، تلك العملية التي يمكن من خلالها التحقق من هوية الشخص الذي يمارس نشاطه عبر الشبكة مع شخص آخر، فالطبيعي أن تكون التجارة محاطة بالثقة عند إبرام العقد التجاري، لتسهيل التحقق من هوية الأطراف، إلا أن هذه الثقة

قد تكون محدودة أو مهددة بعدم الصحة في الوسائل الإلكترونية، الأمر الذي قد يتشكك منه المستهلك، فيلجأ إلى البحث عن كل حماية للطمأنينة بشأن مدى إمكانية تنفيذ الطرف الآخر لالتزامه القانوني، ومدى قدرة أمن الاتصالات الإلكترونية في تحقيق المصدقية.⁵

من ناحية أخرى، إن معرفة هوية المتعاقد الآخر عنصر هام في الروابط العقدية وذلك لتعيين القانون الواجب التطبيق عندما يكون هذا الأخير هو القانون الشخصي للأطراف وإذا كانت هناك وسائل لتحديد هوية المتصل معه، مثل برامج مقتفي الأثر إلا أنها من الناحية العملية معقدة بالنسبة لغالبية المستخدمين.⁶

يلجأ المتعاملين الإلكترونيين خاصة البنوك في سبيل تحقيق هذا الأمان إلى تقنيات يسعى من خلالها إلى التأكد من مشروعية الاستفادة من خدماتها وأن المستفيد فعلاً هو العميل صاحب الحساب.⁷

وعليه سنتطرق إلى تحديد نظام هوية المستخدم وكلمة السر في الفرع الأول، ثم سنتطرق إلى تحديد نظام كلمة السر التي لا تتكرر في الفرع الثاني.

الفرع الأول: تحديد نظام هوية المستخدم وكلمة السر

عند دخول العميل إلى الموقع قصد الاستفادة من الخدمات الإلكترونية، أول ما يصادفه هو إدخال هوية المستخدم وكلمة السر، إلا أنه رغم الاحتياطات التي يتخذها المتعامل من أجل عدم كشف كلمة السر الخاصة به، فإن ابتكارات بعض الأشخاص الذي يحترفون الإجرام عبر الانترنت تجعلهم قادرين على التوصل لمعرفتها وهذا أمر خطير بالنسبة للحسابات البنكية بحيث يتمكن المجرم من تحويل أموال إلى حسابات أخرى دون أن يترك أي أثر عن هويته، وذلك باستخدام أساليب تقنية للاقتحام والسطو، ولعل أكثر على كلمات السر هو أسلوب الاقتحام العشوائي أو التخمين العشوائي، بحيث يقوم المقتحم بتجربة كل القيم الممكنة وقد ظهرت على الانترنت مجموعة من البرامج تقوم بهذه المهمة بسرعة فائقة مثل برنامج crack lophet وهو برنامج للتخمين العشوائي سريع جداً.⁸

الفرع الثاني: تحديد نظام كلمة السر التي لا تتكرر

وقد سميت هذه الطريقة بكلمة السر التي لا تكرر لأن كلمة السر لا تكون صالحة إلا مرة واحدة، تستخدمه خاصة البنوك عند إجراء العمليات التي تتضمن أوامر الدفع، يستخدم هذا النظام كوسيلة إضافية للنظام السابق حيث يعتمد على اشتراك كل من العميل والبنك للتوصل لكلمة السر التي لا تكرر، حيث يتم تزويد كل منها في البداية بنفس جملة المرور وعدد مرات إدخال

البيانات الخوارزمية القيمة الاختيارية،⁹ فيبدأ العميل بإرسال رسالة البداية فيرد البنك برقم عشوائي يتم استخدامه في إخراج كلمة السر التي لا تكرر، ويمر كل ذلك بثلاث خطوات:

أولاً: الخطوة التمهيدية

يدخل العميل جملة المرور ويتم إضافته إلى الرقم العشوائي ثم ترسل إلى البنك.

ثانياً: خطوة التوليد

يتم تنفيذ خوارزمية القيمة الاختيارية عدة مرات على هذه الجملة لإنتاج كلمة سر ذات 64 خانة أو أكثر، هذا العدد هو المخزن في جهاز العميل والبنك.

ثالثاً: خطوة العرض

حيث تأخذ كلمة السر المنتجة في المرحلة السابقة وتعرض بصورة مقروءة، وفي المرحلة النهائية يستخدم العميل هذه الكلمة مرة واحدة فقط بإرسالها للبنك.

الذي يتأكد من صحتها بعد أن تتم العملية المراد إنجازها، تصبح هذه الكلمة غير صالحة للاستعمال.

المطلب الثاني

تقنية أمن المراسلات والمواقع الإلكترونية

تهدف هذه التقنيات إلى تأمين وصول البيانات المطلوبة دون زيادة أو نقصان في صورة سليمة وصحيحة إلى المرسل إليه المعني دون غيره في الوقت المحدد لها دون تأخير،¹⁰ فخاصية افتتاح شبكة المعلومات أمام جميع مستخدميها سواء الكاشفين عن هويتهم أو مخفيها يهدد سرية البيانات المتبادلة بين الأطراف.¹¹

وتتعلق هذه الصعوبات بالنواحي الفنية الخاصة بتكنولوجيا المعلومات والاتصالات والبرمجيات وأنظمة التشغيل، هذا ما أدى بالعاملين في الميدان الإلكتروني إلى ابتكار وسائل حديثة لحماية أمن وسرية المراسلات والمعلومات عن طريق تشفيرها، وحماية المواقع الإلكترونية من خلال جدران الحماية.

وعليه سنتطرق في هذا المطلب إلى التشفير في الفرع الأول، ثم سنتطرق إلى جدران الحماية في الفرع الثاني.

الفرع الأول: التشفير

يعرف التشفير بأنه تحويل المعلومات إلى شفرات غير مفهومة (دون معنى) لمنع الأشخاص غير المرخص لهم من الاطلاع على المعلومات وحفظها من العبث بمحتويات وذلك بتغيير شكلها إلى

صورة لا يمكن فهمها إلا بعد إرجاعها إلى صورتها الأصلية، فعملية التشفير تعمل على تحويل النصوص العادية إلى نصوص مشفرة وذلك باستخدام مفاتيح وهذه المفاتيح تستند إلى صيغ رياضية معقدة (خوارزميات) وتعتمد قوة وفعالية التشفير على أساسين: الخوارزمية وطول المفتاح (مقدر بالبت Bit)،¹² وينقسم التشفير إلى متماثل، وتشفير لا متماثل.

أولاً: التشفير المتماثل

هو 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.¹³

ثانياً: التشفير اللامتماثل

وهو أسلوب من أساليب التشفير، يتم فيه تشفير البيانات باستخدام مفتاح ما، وفك تشفيرها باستخدام مفتاح آخر، ولهذا السبب يسمى بالتشفير بالمفتاح اللامتناظر، لأن مفتاح التشفير يختلف عن مفتاح فك التشفير وهذا هو الفرق بين التشفير المتناظر والتشفير اللامتناظر، حيث أنه في التشفير المتناظر يتم تشفير الرسالة أو التوقيع باستخدام الرقم العام وفي نفس الوقت يتم فك الشفرة وإرجاء المعلومات إلى وضعها الأصلي باستخدام نفس الرقم العام، ولو حصل أن الشخص 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 اللامتناظر 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.¹⁴

وفي هذا الإطار ويهدف 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 أما القانون الصادر بتاريخ 26 جويلية 1996 قام بتحرير 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 أحد الأشخاص 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 أحد الأشخاص ذوي الثقة، لأن الاستعمال الشخصي لهذه الوسائل والخدمات يكون خاضعا لترخيص صادر عن السلطة الحكومية العليا.¹⁵

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،¹⁶ بالإضافة إلى تشفير مستوى التصفح باستخدام NET ESCAPE للتأمين SSI.¹⁷

أ - نظام المعاملات الإلكترونية الأمانة SET

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

ويتميز هذا النظام،¹⁸ عن الأنظمة التأمينية الأخرى بعدة مميزات كونه:

1. يضمن أن طلب الشراء المرسل هو نفسه الطلب الذي يستقبله صاحب المشروع أو التاجر عن طريق بصمة ورقية معينة تكون مميزة لهذا الطلب.
2. يضمن سرية طلب الشراء عن طريق تشفير المعلومات التي يشملها الطلب وكذلك البيانات الخاصة بعمليات الوفاء.
3. يضمن للتاجر أو صاحب المشروع، أن حامل البطاقات 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 الرقم الحساب المذكور، كما أنه يعطي للتاجر ضمان بأن حساب المشتري يسمح بشراء هذه السلعة أو الخدمة المراد شرائه دون معرفة البائع برقم البطاقة البنكية الخاصة بالمشتري.

ب - نظام للتأمين SSL

وتمكن مهمة البروتوكول في تشفير جميع الاتصالات بأحد برامج التصفح أو النوافذ على شبكة المعلومات (BROWSER) أو أحد 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 المعلومات والبيانات الخاصة بهم بما فيها إتمام البطاقة البنكية لن تكون متاحة سوى للتاجر أو المنشأ أو المؤسسة المراد التعامل معها وذلك للتأمين البطاقة البنكية.¹⁹

تحتاج عملية التشفير إلى طرف ثالث محايد لضمان الأمان، فمثلا في تونس يمكن لأي شخص طبيعي أو معنوي أن يمارس عملية التشفير في نطاق التجارة والمبادلات الإلكترونية، بشرط أن يتحصل على تصريح مسبق من الوكالة الوطنية للمصادقة الإلكترونية،²⁰ كذلك في مشروع قانون التجارة الإلكترونية المصري، بحيث نص في فصله الخامس على إنشاء مكتب للتشفير يكون جهة لإيداع مفاتيح الشفريات.

في القانون الجزائري بالرجوع إلى المرسوم التنفيذي رقم 98-257 المتعلق باستغلال خدمات الانترنت المعدل والمتمم، استعمل المشروع مصطلح " الترميز " في فحوى المادة 14 التي تنص على: "يلتزم مقدم خدمات الانترنت خلال ممارسة نشاطه بما يلي... - عرض أي مشروع خاص باستعمال الترميز على اللجنة"، وذكر نفس المصطلح في نص المادة 07 من المرسوم التنفيذي رقم 09-410 مؤرخ في 10 ديسمبر 2009 يحدد قواعد الأمن المطبقة على النشاطات المنصبة على التجهيزات الحساسة،²¹ ومحتوى هذا النص يلزم بوجود الحصول على اعتماد مسبق من المصالح المكلفة بوزارة الداخلية بعد استشارة السلطة المؤهلة المكلفة بالمصادقة على تجهيزات وبرامج الترميز قصد ممارسة نشاط الترميز.

يفهم من هذا النص أن مقدم خدمات الانترنت يقترح على الوزارة مشروعات خاصة بالترميز أو التشفير.

وذكرها المشرع الجزائري في قانون رقم 18-05 في المادة 06 البند 08 بمصطلح اسم النطاق: " عبارة عن سلسلة أحرف و أو أرقام مقتبسة ومسجلة لدى السجل الوطني لأسماء النطاق، وتسمح بالتعرف والولوج إلى الموقع الإلكتروني".²²

بالإضافة إلى تقنية التشفير نجد تقنية أخرى تعمل على أمن المراسلات والمواقع الإلكترونية ألا وهي جدران الحماية.

الفرع الثاني: جدران الحماية

تدعى كذلك بالجدار النارية،²³ وتعتبر وسيلة تستعمل لحماية الشبكات الخاصة من الدخول وتمنع الوصول الغير مشروع به للشبكة حيث تحمي وحدات التحكم والإرسال في الانترنت.

وتتجلى أهمية الجدران النارية في حماية الشبكات الخاصة من هذه المشكلات، حيث أنه وعبر الانترنت يتم التعامل على بث متعدد الأطراف باستعمال الأجهزة السمعية والبصرية ومؤتمرات الفيديو لمجموعة من المضيفين ليرى ويسمع كل منهم الآخر، ويوفر الهيكل الإذاعي المتكامل على الانترنت عن طريق برنامج (MPHONE) المتوافر لكل الناس حيث أن أي مستعمل في الانترنت

يستعمل في هذا الجهاز (MPHONE) يتيح المجال لأي مستعمل آخر للدخول عليه ومراقبته في الانترنت ولكن الجدار الناري يمنع هذا الدخول.²⁴

وهذه الوسائل لا تكفي وحدها لحماية أمن المعلومات بشكل كامل، بل لا بد من استخدام تقنيات الأمن الشامل التي تضم العديد من الأجهزة والنظم مثل الوسائل أمن الملفات ووسائل كشف الاقتحام وأجهزة الرقابة.²⁵

المبحث الثاني

تأمين الدفع الإلكتروني

إن حماية المستهلك عند الدفع الإلكتروني ترتبط بالعديد من الأمور، فتسوق المستهلك عبر الانترنت وقيامه بالتعاقد أو الشراء يرتبط بالدفع الإلكتروني، لذلك فالأجهزة الإلكترونية وثيقة الصلة بالتعاقد الإلكتروني، ويمكن عن طريق هذه الصلة تحويل المبالغ لحسابات أخرى، ودفع الفواتير، لجهات خارج البنك من خلال الدفع الإلكتروني الذي يتم من خلال بطاقات الدفع الإلكتروني أو بطاقات الائتمان التي تخول صاحبها بتحويل قيمة مالية معنية من حسابه إلى حساب البائع.²⁶

وعليه سنتطرق في هذا المبحث إلى التأمين الفني لعملية الدفع الإلكتروني في المطلب الأول، ثم سنتطرق إلى التأمين القانوني لعملية الدفع الإلكتروني في المطلب الثاني.

المطلب الأول

التأمين الفني لعملية الدفع الإلكتروني

يتحقق هذا التأمين من خلال الوظائف والشروط الفنية التي يجب أن تتوفر في عملية الدفع كي تكون آمنة، وتمثل هذه الشروط في إضفاء الصفة الرسمية على الأمر بالدفع إلى الجانب تقنية التشفير والتميز وحفظ المعلومات الخاصة بعملية الدفع وكذا تحديد التاريخ الإلكتروني لواقعه الدفع.²⁷

وعليه سنتطرق إلى إضفاء الصفة الرسمية على الأمر بالدفع في الفرع الأول، ثم سنتطرق إلى التأمين القانوني لعملية الدفع الإلكتروني في الفرع الثاني.

الفرع الأول: إضفاء الصفة الرسمية على الأمر بالدفع

يتم إفراغ التصرفات القانونية في التجارة التقليدية أو اليدوية في مستندات مكتوبة يتم تذيلها بتوقيع من صاحب الشأن، هذا على خلاف الحال في التجارة الإلكترونية حيث يتم إبرام الصفقات على دعائم الكترونية غير مكتوبة تقليديا ويتم التوقيع عليها من قبل أطراف الصفقة

الإلكترونية. وإذا كان من السهل الرجوع إلى المستندات الورقية والتحقق من صحة ونسبة صدور التصرف إلى موقعه، فإن الأمر ليس بنفس السهولة بالنسبة للمستندات الإلكترونية بما تحمله من توقعات الكترونية والتي هي بحاجة إلى من يوثقها ويصادق عليها.²⁸

الفرع الثاني: حفظ المعلومات الخاصة بعملية الدفع الإلكتروني:

يشكل الحفظ وسيلة هامة لتأمين الوفاء الإلكتروني، وهو يعني حفظ المستندات أو المعلومات المتعلقة بعملية الوفاء بطريقة لا يمكن محوها ولأكبر فترة ممكنة لإمكانية الرجوع إليها كلما دعت الضرورة لذلك.

فالمنهج أو الطريقة التي تنتجها أنظمة بطاقات السحب من أجل تأمين المستندات والمعلومات و المعاملات المصرفية والدفع الإلكتروني، تجعل هذه الطريقة أكثر صعوبة في التعامل من العملات الورقية والمعدنية، فعندما يقوم صاحب البطاقة بتقديم بطاقته إلى البائع من أجل الشراء، فإن مسجل النقد الإلكتروني التابع للمزود يقوم بإرسال رسالة طلب التحويل إلى بنك المستهلك، ومن ثم يقوم بنك المستهلك بالكشف عن حساب المستهلك، والتأكد من وجود إيداع مصرفي كافٍ من أجل انجاز المعاملة، وأيضا يقوم البنك بالكشف على سجل من الأرقام من أجل التأكد من أن تلك البطاقة ليست مسروقة أو ضائعة، فإن كانت الأمور على ما يرام، فإن بنك المستهلك يرسل رسالة إلى المزود تؤكد له قدرة المستهلك على الدفع، ونظام التأكد هذا ما بين المزود وبنك المستهلك يعزز من أمن النظام لصالح صاحب البطاقة، ولصالح المزود، وبالتالي تعزز الثقة لدى المستهلك.

وعليه تعرض المجلس الأوروبي لموضوع حماية المستهلك عند الدفع الإلكتروني تحت مسمى تأمين نظام الوفاء، حيث صدرت توصية عن المجلس الأوروبي في 19/05/1998 بهدف المساهمة في إنعاش التجارة الإلكترونية، عن طريق زيادة ثقة المتعاملين فيها وفي أساليها، خاصة السداد الإلكتروني، وبحث سبل حماية المستهلك والتاجر عند السداد بهذه الطريقة، وكيفية إمكان الاسترداد في حالة السداد بدون وجه حق، وكيف تتم الحماية من المخاطر في حالة سرقة البطاقة أو فقدانها أو ضياعها.³⁰

وهذا ما أكدته المشرع الجزائري في قانون رقم 18-05 في الفصل السادس تحت عنوان الدفع في المعاملات الإلكترونية في المواد 27-28-29 من أجل تأمين وسائل الدفع الإلكترونية، وتنص المادة 27 من نفس القانون، (يتم الدفع في المعاملات التجارية الإلكترونية إما عن بعد أو عند تسليم المنتج، عن طريق وسائل الدفع المرخص بها، وفقا للتشريع المعمول به).

عندما يكون الدفع الكترونيا، فانه يتم من خلال منصات دفع مخصصة لهذا الغرض، منشأة ومستغلة حصريا من طرف البنوك المعتمدة من قبل بنك الجزائر و بريد الجزائر وموصولة بأي نوع من أنواع محطات الدفع الإلكتروني عبر شبكة المتعامل العمومي للمواصلات السلكية واللاسلكية.

يتم الدفع في المعاملات التجارية العابرة للحدود، حصريا عن بعد، عبر الاتصالات الإلكترونية).

ومن أجل التأكيد على حماية المستهلك عبر الاتصال الإلكتروني في مجال المعاملات التجارية، عبر منصة الدفع الإلكترونية، يجب أن تكون مؤمنا بواسطة نظام تصديق الكتروني، موصول بكل من أطراف التعاقد المورد والمستهلك عبر شبكة الانترنت عن طريق منصة الدفع الإلكترونية لحماية خصوصية البيانات عبر الشبكة الإلكترونية، هذا ما نصت عليه المادة 28 من قانون التجارة على أنه (يجب إن يكون وصول موقع الانترنت الخاص بالمورد الإلكتروني بمنصة الدفع الإلكترونية مؤمنا الكترونيا)، وهذا النص يؤكد على حماية وسائل الدفع الإلكتروني عندما تكون موصولة بمنصات الدفع الإلكترونية المؤمن من طرف البنك والجهات المختصة.

وعليه عند العملية الشرائية فإن مسجل النقد الإلكتروني يقوم بتسجيل قيمة البيع وتخزينها مع تسجيل اسم الجهة المصدرة للبطاقة، وفي وقت لاحق أو في نفس الوقت، يقوم البائع بإرسال بيانات المعاملات المسجلة إلى البنك الذي يمتلك حسابه، ومن ثم يقوم بنك البائع بمطالبة المستحقات من بنك المستهلك أو صاحب البطاقة، وعندما يرسل بنك المستهلك موافقته لرد المستحقات، فإن بنك البائع يزيد رصيد الحساب للبائع، كما تكون هذا المعاملات محمية من طرف البنك الخاص بهذا المعاملات.³¹

ونصت المادة 29 من قانون رقم 18-05 المتعلق بالتجارة الإلكترونية الجزائري على ما يلي (تخضع منصات الدفع الإلكتروني المنشأة المستقلة طبقا للمادة 27 أعلاه، لرقابة بنك الجزائر لضمان استجابتها لمتطلبات التشغيل البيئي وسرية البيانات وسلامتها وامن تبادلها).³²

وكما أنه صدر عن بنك الجزائر قانون رقم 05-07 مؤرخ في 28 ديسمبر 2005، متعلق بأمن أنظمة الدفع حيث نظم أمن عمليات التسوية المالية دون أن يشير لطرق الدفع الإلكترونية،

إذ نص في المادة 12 منه على "يسهر بنك الجزائر على توفير الأمن المادي والمنطقي للبنية الأساسية الخاصة بأنظمة الدفع، كما يتأكد من توفير أمن وسائل الدفع من غير العملية النقدية في هذا المجال.

وفي حالة ما إذا اعتبر بنك الجزائر بأنه يتوفر في إحدى وسائل الدفع على الضمانات الأمنية، يمكن أن يطلب من الجهة التي تصر اتخاذ إجراءات ملائمة لمعالجة الأمر، وفي حالة عدم تطبيق هذه التوصيات يمكنه بعد استشارة السلطة المكلفة بالمراقبة في اتخاذ قرار توقيف إدخال وسيلة الدفع المعنية في النظام.

يتعين على بنك الجزائر بصفة خاصة، التأكد من أمن بطاقات الدفع ومتابعة إجراءات توفير شروط الأمن التي قامت بها الجهات التي تصدرها، وكذا التجار ومتابعة إحصاءات التدليس والتطورات في ميادين التكنولوجيا، التي قد تؤثر على أمن بطاقات الدفع".³³

يتضح لنا من خلال هذه المادة أن المشرع الجزائري ألزم الأشخاص الذي يريدون إدخال وسائل أمن حديثة بتأمينها حماية للمتعاملين، كما منح بنك الجزائر سلطة الرقابة وألزمه في الوقت نفسه بالسهر على متابعة التطورات التي تؤثر على أمن بطاقات الدفع بغرض تعزيز العمل بهذه البطاقات.³⁴

الفرع الثالث: تحديد التاريخ الإلكتروني

تظهر ضرورة تاريخ المستند الإلكتروني في عدة نقاط منها:

أولاً: تحديد فيما إذا كان هناك تأخير في تنفيذ العقد ومن ثم تطبيق الجزاءات المفروضة على التأخير في التنفيذ وما يترتب على هذا التأخير من مصاريف جمركية إضافة نتيجة للتأخير في تخليص البضاعة جمركياً.³⁵

ثانياً: يجب أن تكون الوسيلة مشمولة بضمانات تضمن للتاجر حصوله على الثمن كاملاً دون أن يتحمل مخاطر عدم ملاءة المشتري وذلك عن طريق خطابات الضمان أو الكفالة المصرفية مثلاً.

ثالثاً: ضمان عدم اعتراض مصدر الأمر بالوفاء على عدم وجوده أو بطلانه وهو ما يتطلب إقامة نظام فعال للإثبات.

المطلب الثاني

التأمين القانوني لعملية الدفع الإلكتروني

تأخذ عملية تأمين الدفع بالنسبة للمستهلك بعدين، يتمثل البعد الأول في البحث عن وسيلة تضمن له عدم السحب من رصيده المتاح بموجب وسيلة الدفع المستخدمة إلا المبالغ

المتفق عليها،³⁶ وذلك يستدعى تفعيل مسؤولية البنك عن الأخطاء التقصيرية أو التعاقدية التي من شأنها الإضرار بالعميل وعدم تحميل العميل مخاطر تشغيل النظام المعلوماتي مع التأكد من صحة أمر الدفع، ومن أجل حماية وسائل الدفع يجب على كل من العميل والمستهلك بالدفع ضمن الوسائل المرخص بها، وفقاً للتشريع المعمول به، وهذا ما أكدته المادة 27 من قانون رقم 05-18 المتعلق بالتجارة الإلكترونية.

أما البعد الثاني يتمثل في إقامة نظام يربط بين لحظة الدفع ولحظة التسليم، وهذا ما نصت عليه المادة 28 من نفس القانون على أنه : (يجب أن يكون وصل موقع الانترنت الخاص بالموارد الإلكتروني بمنصة الدفع الإلكتروني مؤمناً بواسطة نظام تصديق الكتروني وعليه يعد التوقيع على وسائل الدفع الإلكترونية وسيلة لتوطيد الثقة وبعث الطمأنينة في مجال المعاملات الإلكترونية عامة والتجارة الإلكترونية خاصة، لهذه الأسباب وغيرها سارعت التشريعات المقارنة إلى تقنين التوقيع الإلكتروني والتشجيع التعامل عبر منصات الدفع الإلكتروني وإبراز دوره القانوني والمتمثل في تعيين صاحب التوقيع أولاً والتعبير عن قبوله للالتزامات الدفع عبر منصات الدفع الإلكتروني التي يضمها ويحميها القانون من خلال مجموعة من النصوص القوانين وأمن التقنيات.

خاتمة

وخلاصة القول نقول أن المشرع الجزائري حسم أمره في تأمين وحماية وسائل الدفع من خلال صدور قانون التجارة الإلكتروني الجزائري رقم 05/18، الذي حدد فصل السادس من هذا القانون تحت عنوان الدفع في المعاملات الإلكترونية، وهذا من أجل تشجيع التعامل بالمعاملات الإلكترونية بصفة عامة ووسائل الدفع الإلكتروني بصفة خاصة، وعمل على تأمين الحماية لها، وذلك من خلال ربط منصات الدفع الإلكتروني الخاصة بالموارد بنظام تصديق إلكتروني مؤمناً. وقد توصلنا إلى نتائج وتوصيات هذه الدراسة إلى النتائج والتوصيات:

أولاً: النتائج:

1. يتم الدفع في المعاملات التجارية الإلكترونية عن طريق وسائل الدفع المرخص بها، وفقاً للتشريع المعمول به.
2. حماية البيانات والمعلومات من خلال عملية تشفير المعلومات من أجل تأمين عمليات الدفع عبر المواقع الإلكترونية من خلال عمليات تصديق مؤمناً مرتبط بالبنك الجزائري وهي الجهة المكلفة برقابة وحماية المعلومات والبيانات .

3. تخضع منصات الدفع الإلكتروني لرقابة بنك الجزائر لحماية البيانات وسلامتها وأمن تبادلها.
 4. تخضع منصات الدفع الإلكتروني الخاصة بالموارد لنظام تصديق إلكتروني مؤمنا.
- ثانيا: التوصيات:

1. توصي الدراسة بتوسيع نطاق الرقابة إلى هيئات مختصة تتنبأ وقوع عمليات اختراق لحسابات المورد أو المستهلك أو البنك المراقب نفسه، وذلك من خلال الإجراءات الإستباقية تقوم بها مع الجهات المعنية بالأمر، من أجل تفادي وقوع الجرائم.
2. توصي هذه الدراسة بإنشاء هيئات تعمل على تعليم المستهلك كيفية استعمال وسائل الدفع الإلكتروني، وكيفية حمايته من المخاطر، ورشاده وتوجيهه وتعريفه بمنصات المرخص بها من أجل حمايته ونشر الثقة لجمهور المستهلكين.
3. توصي الدراسة بتوسيع نطاق التعامل بوسائل الدفع الإلكتروني في كل مؤسسات التجارية والأسواق المحلية بمختلف أنواعها، وذلك من خلال تشجيعها وتدعيمها بأجهزة ووسائل الدفع إلكترونية، وذلك من خلال إنشاء مؤسسات خاصة تعمل على تشجيع التعامل بدفع الإلكتروني وحمايتها في نفس الوقت، وترشدهم على كيفية استخدام وسائل الدفع.

قائمة المصادر والمراجع

1- المراجع باللغة العربية

أولاً: الكتب:

- أمينة أحمد محمد أحمد، حماية المستهلك في عقود التجارة الإلكترونية، دراسة مقارنة، دار النهضة العربية، مصر، 2016.
- حسن طاهر داوود، الحاسب وأمن المعلومات، معهد الإدارة العامة، السعودية، 2000.
- سامي عبد الباقي أبو صالح، الوفاء الإلكتروني بالديون الناشئة عن المعاملات التجارية، دار النهضة العربية القاهرة، مصر 2006.
- سامي عبد الباقي أبو صالح، الوفاء الإلكتروني بالديون الناشئة عن المعاملات التجارية، دار النهضة العربية القاهرة، مصر، 2006.
- عبد الفتاح بيومي حجازي، حماية المستهلك عبر شبكة الانترنت، الطبعة الأولى، دار الفكر الجامعي، مصر، 2006.
- علي كحلون، الجوانب القانونية لقنوات الاتصال الحديثة والتجارة الإلكترونية، دار إسهامات في أدبيات المؤسسة تونس، 2002.

- محمود محمد أبو فروة، الخدمات البنكية الالكترونية عبر الانترنت، دار الثقافة، الأردن، 2009.

ثانياً: المذكرات:

- خلود (عنان) نصيرة، حماية المستهلك عبر الانترنت (دراسة مقارنة)، أطروحة مقاومة لنيل شهادة الدكتوراه علوم، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، تاريخ المناقشة، 2018/07/02.
- حابت أمال، التجارة الالكترونية في الجزائر، أطروحة لنيل درجة دكتوراه في العلوم، تخصص قانون، جامعة مولود معمري، ولاية تيزي وزو، 30 سبتمبر 2015.
- فيصل محمد محمد كمال عبد العزيز، الحماية القانونية لعقود التجارة الالكترونية، رسالة لنيل درجة الدكتوراه في القانون التجاري، جامعة القاهرة، 2008.
- عمر هبطي، التوقيع الإلكتروني، رسالة لنيل دبلوم الدراسات العليا المعمقة في القانون الخاص، وحدة التكوين والبحث، قانون الأعمال، جامعة الحسن الثاني، كلية العلوم القانونية والاقتصادية والاجتماعية، عين الشق، الدار البيضاء، المغرب، السنة الجامعية، 2006/2007.
- عبد الله ذيب عبد الله محمود، حماية المستهلك في التعاقد الإلكتروني دراسة مقارنة، رسالة ماجستير، جامعة النجاح، نابلس، فلسطين، جامعة النجاح، نابلس، فلسطين، 2009.
- حابت أمال، التجارة الإلكترونية في الجزائر، أطروحة لنيل درجة الدكتوراه، جامعة مولودي معمري، ولاية تيزي وزو، الجزائر، 2015.

ثالثاً: المجالات:

- حسن عبده الماحي، نظرات قانونية في التجارة الالكترونية، مجلة البحوث القانونية والاقتصادية بكلية الحقوق، جامعة المنصورة، العدد 31، أبريل 2002.
- حمودي ناصر، التنظيم القانوني لظاهرة العولمة في الجزائر، الانجازات والتحديات، المجلة النقدية للقانون والعلوم السياسية، كلية الحقوق، جامعة مولود معمري، تيزي وزو، عدد 02، 2012.

رابعاً: المقالات:

- محمد بن أحمد السيدري، مقالة بعنوان التجارة الالكترونية تقنيات واستراتيجيات التطبيق، منشورة في الموقع الإلكتروني <http://faculty.ksu.edu.sa/mas/published> تاريخ 2019/3/2 الساعة 8:11 م.
- ضياء على أحمد نعمان، الحماية التقنية للتجارة الالكترونية، مقال منشور بمجلة قانون وأعمال، العدد الأول، المغرب، 2011.

خامساً: المداخلات:

- يونس عرب، مداخلة منشورة على الموقع الإلكتروني بعنوان: التعاقد والدفع الالكتروني تحديثات النظامين الضريبي والجمركي مقدمة إلى برنامج الندوات المتخصصة حول التجارة الالكترونية، تنظيم معهد التدريب والإصلاح القانوني، الخرطوم، كانون الأول 2002، متوفر على الموقع التالي: <http://www.f-law.net>، تاريخ 2019/2/30 الساعة 11:10 م.

سادساً: المواد:

- قانون التجارة والمبادلات الالكترونية التونسي رقم 83 لسنة 2000.
- قانون رقم 10-05 المتعلق بالتجارة الالكترونية الجزائري الصادر في 16/مايو 2018
- قانون رقم 07-05 المتعلق بأمن أنظمة الدفع المؤرخ في 28 ديسمبر 2005 الصادر في الجريدة الرسمية عدد 37/2006.

2- المراجع بالفرنسية:

- BERBAN Yan et POTTIER Isabelle, les décrets et antes cryptologies la mise en œuvre effective de l'assouplissement des dispositions antérieure, revue de la gazette du plais n° 103 a 11 du 19 au 21 avril 1998.
- Muriel falaise, réflexions sur l'avenir du contrat du commerce électronique, petite affiche, n° 94, 7 aout 1998.

الهوامش:

- ¹. خلود (عنان) نصيرة، حماية المستهلك عبر الانترنت (دراسة مقارنة) ، أطروحة مقاومة لنيل شهادة الدكتوراه علوم، كلية الحقوق والعلوم السياسية، جامعة مولود معمور، تيزي وزو، تاريخ المناقشة، 2018/07/02، ص 218.
- ². أمينة أحمد محمد أحمد، حماية المستهلك في عقود التجارة الإلكترونية، دراسة مقارنة، دار النهضة العربية، مصر، 2016، ص 216.

- ³. نظام رقم 08/11 المؤرخ في 28 نوفمبر سنة 2011، يتعلق بالرقابة الداخلية للبنوك و المؤسسات المالية الصادر في الجريدة الرسمية العدد 47، سنة 2012.
- ⁴. Muriel falaise, réflexions sur l'avenir du contrat du commerce électronique, petite affiche, n° 94, 7 aout 1998, p 5.
- ⁵. حسن عبده الماحي، نظرات قانونية في التجارة الالكترونية، مجلة البحوث القانونية والاقتصادية بكلية الحقوق، جامعة المنصورة، العدد 31، أبريل 2002، ص 294.
- ⁶. فيصل محمد محمد كمال عبد العزيز، الحماية القانونية لعقود التجارة الالكترونية، رسالة لنيل درجة الدكتوراه في القانون التجاري، جامعة القاهرة، 2008، ص 50.
- ⁷. حابت آمال، التجارة الالكترونية في الجزائر، أطروحة لنيل درجة دكتوراه في العلوم، تخصص قانون، جامعة مولود معمري، ولاية تيزي وزو، 30 سبتمبر 2015، ص 275.
- ⁸. محمود محمد أبو فروة، الخدمات البنكية الالكترونية عبر الانترنت، دار الثقافة، الأردن، 2009، ص 87.
- ⁹. البيانات الخوارزمية: هي عبارة عن مجموعة من العمليات الحسابية يتم من خلالها توليد مجموعة من الحروف ذات طول معين مستنتجة رياضيا من مجموعة أخرى من الحروف أطول بكثير والتي تمثل الرسالة المراد تشفيرها، كما تستخدم هذه العملية كذلك لاكتشاف تزوير البيانات، حيث أن أي تغيير ولو كان بسيطا في الرسالة الأصلية يؤدي إلى تغيير كبير في القيمة الاختيارية، راجع محمود أبو فروة، المرجع السابق، ص 88.
- ¹⁰. حسن طاهر داوود، الحاسب وأمن المعلومات، معهد الإدارة العامة، السعودية، 2000، ص 216.
- ¹¹. حسن عبده الماحي، المرجع السابق، ص 295.
- ¹². محمد بن أحمد السيدري، مقالة بعنوان التجارة الالكترونية تقنيات واستراتيجيات التطبيق، منشورة في الموقع الإلكتروني <http://faculty.ksu.edu.sa/mas/published> تاريخ 2019/3/2 الساعة 8:11 م.
- ¹³. علي كحلون، الجوانب القانونية لقنوات الاتصال الحديثة والتجارة الالكترونية، دار إسهامات في أدبيات المؤسسة تونس، 2002، ص 282.
- ¹⁴. عمر هبطي، التوقيع الالكتروني، رسالة لنيل دبلوم الدراسات العليا المعمقة في القانون الخاص، وحدة التكوين والبحث، قانون الأعمال، جامعة الحسن الثاني، كلية العلوم القانونية والاقتصادية والاجتماعية، عين الشق، الدار البيضاء، المغرب، السنة الجامعية، 2006/2007، ص 109.
- ¹⁵. BERBAN Yan et POTTIER Isabelle, les décrets et antes cryptologies la mise en œuvre effective de l'assouplissement des dispositions antérieure, revue de la gazette du plais n° 103 a 11 du 19 au 21 avril 1998. P 12.
- ¹⁶. SET: Secure électronique transaction.
- ¹⁷. SSI: Secure socket layer.
- ¹⁸. تم تطوير نظام المعلومات الالكترونية الأمانة SET بالتعاون بين أكبر شركات البطاقات البنكية وهما VISA و MASTER CARD وذلك بغرض تأمين المعاملات المالية عبر شبكة الانترنت باستخدام البطاقة البنكية، راجع ضياء على أحمد نعمان، الحماية التقنية للتجارة الالكترونية، مقال منشور بمجلة قانون وأعمال، العدد الأول، المغرب، 2011، ص 40.

- ¹⁹. ضياء على أحمد نعمان، مقالة بعنوان الحماية التقنية للتجارة الإلكترونية منشورة بمجلة القانون والأعمال، العدد الأول، المغرب، 2011، ص 33.
- ²⁰. قانون التجارة والمبادلات الالكترونية التونسي، رقم 83 لسنة 2000.
- ²¹. المرسوم التنفيذي رقم 09-410 مؤرخ في 10 ديسمبر 2009 يحدد قواعد الأمن المطبقة على النشاطات المنصبة على التجهيزات الحساسة، الصادر في الجريدة الرسمية عدد 73 لسنة 2009.
- ²². قانون رقم 10-05 المتعلق بالتجارة الالكترونية الجزائري الصادر في 16/ مايو 2018.
- ²³. الجدار الناري: هو مجموعة أنظمة توفر سياسات أمنية بين الانترنت وشبكة المؤسسة وتجبر عمليات العبور إلى الشبكة والخروج منها أن تمر من خلال الجدار الناري الذي يصد المستعملين المتطفلين.
- ²⁴. ضياء علي أحمد نعمان، المرجع السابق، ص 39.
- ²⁵. حابت آمال، التجارة الإلكترونية في الجزائر، أطروحة لنيل درجة الدكتوراه، جامعة مولودي معمري، ولاية تيزي وزو، الجزائر، 2015، ص 279.
- ²⁶. عبد الفتاح بيومي حجازي، حماية المستهلك عبر شبكة الانترنت، الطبعة الأولى، دار الفكر الجامعي، مصر، 2006، ص 79.
- ²⁷. حابت آمال، المرجع السابق، ص 280 وما بعدها.
- ²⁸. سامي عبد الباقي أبو صالح، الوفاء الإلكتروني بالديون الناشئة عن المعاملات التجارية، دار النهضة العربية القاهرة، مصر 2006، ص 111.
- ²⁹. يونس عرب، مداخلة منشورة على الموقع الإلكتروني بعنوان التعاقد والدفع الإلكتروني تحديات النظامين الضريبي والجمركي مقدمة إلى برنامج الندوات المتخصصة حول التجارة الالكترونية، تنظيم معهد التدريب والإصلاح القانوني، الخرطوم، كانون الأول 2002، متوفر على الموقع التالي: <http://www.f-law.net>، تاريخ 2019/2/30 الساعة 11:10 م.
- ³⁰. عبد الفتاح بيومي حجازي، حماية المستهلك عبر شبكة الانترنت، مرجع سابق، ص 80.
- ³¹. عبد الله ذيب عبد الله محمود، حماية المستهلك في التعاقد الإلكتروني دراسة مقارنة، رسالة ماجستير، جامعة النجاح، نابلس، فلسطين، جامعة النجاح، نابلس، 2009، ص 89.
- ³². القانون رقم 18-05 المتعلق بالتجارة الالكترونية الجزائري سالف الذكر.
- ³³. قانون رقم 05-07 المتعلق بأمن أنظمة الدفع المؤرخ في 28 ديسمبر 2005 الصادر في الجريدة الرسمية عدد 2006/37.
- ³⁴. حمودي ناصر، التنظيم القانوني لظاهرة العولة في الجزائر، الانجازات والتحديات، المجلة النقدية للقانون والعلوم السياسية، كلية الحقوق، جامعة مولود معمري، تيزي وزو، عدد 02، 2012، ص 196.
- ³⁵. CAPRIOLI ERIC.OP.CIT.
- ³⁶. سامي عبد الباقي أبو صالح، الوفاء الإلكتروني بالديون الناشئة عن المعاملات التجارية، دار النهضة العربية القاهرة، مصر، 2006، ص 131.