

الاستراتيجيات التقنية الدولية لمحاربة الإرهاب الإلكتروني

International technical strategies to combat cyber terrorism

د. عبد الرحمان بليلة *

كلية الحقوق والعلوم السياسية، جامعة البويرة، البويرة 10000، الجزائر،

a.bellila@univ-bouira.dz

مخبر الدولة والإجرام المنظم، مقارنة قانونية وحقوقية بأبعاد اقتصادية واجتماعية

تاريخ الاستلام: 2021/11/07؛ تاريخ القبول: 2024/12/07؛ تاريخ النشر: 2024/12/22

ملخص:

إن المنهجية الدولية المتبعة لحماية البيئة الإلكترونية أضحت ضرورة قصوى في التصدي لمختلف الجرائم الناتجة عن الإرهاب الإلكتروني بالنظر إلى انتشار هذه الظاهرة المصاحبة لتوظيف التكنولوجيا في مشاريعهم وشتى مجالات تحركاتهم، ومن جهة أخرى يتطلب هذا الأمر مواجهة أمنية لمحاصرة ومكافحة هذه الظاهرة التي أصبحت تعيق حماية وتأمين استخدام تكنولوجيا المعلومات والاتصالات في منصة افتراضية تسمح لمختلف الشركات بإنجاز مهمات محددة مثل: البيع والتسويق.

كما أصبحت الوسائل الأمنية في واجهة هذه الظاهرة غير كافية للتصدي لما خلفته من آثار سلبية على الجانب الاقتصادي مما صعب الأمر في مواجهة ما يسمى بالبرمجيات التخريبية بواسطة إعادة شفرتها الأولية لتعديل ما يختص به الحاسوب.

الكلمات المفتاحية: البيئة الإلكترونية؛ الإرهاب الإلكتروني؛ منصة افتراضية؛ البرمجيات التخريبية؛ الشفرة الأولية.

Abstract:

The international methodology used to protect the electronic Environment has become an utmost necessity in confronting the various crimes resulting from electronic terrorism, given the spread of this phenomenon that accompanies the use of technology in their projects

and various areas of their movements. On the other hand, this matter requires a security confrontation to besiege and combat this phenomenon, which has become an obstacle to protecting and securing. The use of information and communications technology in a virtual platform allows various companies to accomplish specific tasks such as: selling and marketing.

The security means to confront this phenomenon have also become insufficient to address the negative effects it has had on the economic side, which makes it difficult to confront the so-called destructive software by rewriting its initial code to modify what is specific to the computer.

Keywords: electronic environment; electronic terrorism; virtual platform; destructive software; initial code.

مقدمة:

إن التصدي لظاهرة الإرهاب الإلكتروني بالعديد من الوسائل المختلفة يهدف إلى حماية النظام الإلكتروني القائم على معلومات وبيانات وطنية ودولية في إطار تعاون دولي ينشر ثقافة الوعي والإعلام لمحاربة الإرهاب الإلكتروني، حيث تعتبر مسألة نشر الثقافة الإلكترونية وزرع الوعي الفكري في غاية الأهمية من جهة، ومن جهة أخرى تشكل خطورة كبيرة للمجتمعات الإنسانية المعاصرة بحكم أنها تساهم في استمرارية نشر الحضارة الإنسانية وتأثيرها الإيجابي لتنوير الرأي العام.

كما أن قصور القوانين والتشريعات الخاصة بالبيئة الإلكترونية أدى إلى تظافر الجهود الدولية للتعاون في مختلف الجوانب التي لها بعد قانوني مرتبط بوسائل تقنية تخدم الاقتصادي الدولي، حيث يتطلب الأمر إعادة النظر في وضع ميكانيزمات إقليمية ودولية في نظام معلوماتي يرقى إلى تفعيل إطار قانوني في جانب تقني إلكتروني لحماية التجارة الإلكترونية، وكذا المواقع الرسمية لشبكة الأنترنت، وأمن المعاملات المالية في البيئة الإلكترونية، والتي تسهل لكل مستخدم شبكة الأنترنت وضع آليات الحفاظ على المعلومات في مواجهة الأخطار المحتملة⁽¹⁾.

(1)- إبراهيم بخي، التجارة الإلكترونية، مفاهيم واستراتيجيات التطبيق في المؤسسة، ديوان المطبوعات الجامعية، الجزائر، 2005، ص 7

لدراسة وتحليل هذا الموضوع نتطرق للاهتمام الذي توليه الدول لمواجهة خطر ظاهرة الإرهاب الإلكتروني الذي قد يؤثر سلباً على التجارة الإلكترونية، والتي تتعدى معاملاتها الحدود الدولية، ولعالجة هذا الموضوع نطرح الإشكالية التالية: إلى أي مدى تتصدى الوسائل التقنية لمحاصرة ظاهرة الإرهاب الإلكتروني بالنظر إلى قصور الجانب الأمني لتوفير حماية كافية؟

المبحث الأول: حماية المعاملات المالية الإلكترونية

إن حماية التجارة الإلكترونية من خطر الإرهاب الإلكتروني في شقه الأمني غير كاف لوضع آليات محددة تعمل على استمرارية تطور الجانب المعلوماتي بفعل توفير حماية أخرى في جانبها الفني والمتمثلة في الوسائل التقنية التي تمنح المستخدم حماية وأمن أكثر قوة، وأبرزها حماية مختلف المعاملات المالية في البيئة الإلكترونية، وكذا حماية المعاملات المالية في البيئة الإلكترونية، وتتحدد مسؤولية البنك القانونية عندما ينفذ هذا الأخير خدمة من خدماته المصرفية كعملية تحويل الأموال إلكترونياً⁽¹⁾

كما يندرج أمن المعاملات المالية الإلكترونية على وجه الخصوص في وسائل وفاء إلكتروني تستخدم فيها ما يسمى بالبطاقة البنكية وهي عبارة عن وسيط وفاء إلكتروني (المطلب الأول)، أما النوع الثاني يتمثل في نقود إلكترونية على شكل حافظة نقود إلكترونية افتراضية (المطلب الثاني) تستخدم في عملية الشراء عبر شبكة الأنترنت

المطلب الأول: وسيط الوفاء الإلكتروني

إن الوسيط الإلكتروني الأبرز في عملية تحويل الأموال والدفع الإلكتروني هو شبكة الأنترنت باعتبارها وسيلة أمان تقنية بين المدين المستفيد من جهة، ومن جهة أخرى الدائن الذي يتولى عملية الدفع⁽²⁾، ومع تزايد أخطار الولوج إلى شبكة الأنترنت للوصول إلى بيانات ومعلومات وخصوصيات الآخرين، وقد يصل بهم الحد إلى التغيير من معطيات معلوماتهم وحساباتهم.

لإجراء عملية الوفاء بين العميل والتاجر بواسطة إجراءات خاصة تتم بين بنكي هذين الأخيرين، حيث تنقل النقود من الحساب الخاص بالمدين إلى حساب الدائن، وتعد هذه

(2) سليمان ضيف الله الزين، التحويل الإلكتروني للأموال ومسؤولية البنوك القانونية، دار الثقافة للنشر والتوزيع،

الأردن، 2012، ص 127

(3) لزعر وسيلة، تنفيذ العقد الإلكتروني، مذكرة لنيل شهادة الماجستير في القانون، فرع العقود والمسؤولية، كلية الحقوق، جامعة الجزائر (1)، بن عكنون، 2010، ص 185.

العملية أهم أنظمة التحويل الإلكتروني للأموال بين حسابات العميل والتاجر، ونظرا لاستقطاب شبكة الأنترنت عدد كبير من المتعاملين عبرها من كل أقطار العالم تبقى احتمالية سرقة رقم البطاقة عند عملية الدفع الإلكتروني عبر شبكة الأنترنت ممكنة الحدوث، باعتبار أن عملية الدفع تحصل في بيئة إلكترونية معلوماتية مفتوحة قد تحدث فيها أمور غير محددة المعالم⁽¹⁾.

الفرع الأول: النظام الافتراضي الأولي (First virtual)

يعد هذا النظام من أهم أنظمة الوفاء الإلكتروني، حيث نشأ في أمريكا ويشترط أن يكون للتاجر حساب بنكي في أحد البنوك الأمريكية، فيقوم العميل بإجراءات معينة قصد الحصول على حساب بنكي وبعد ذلك يرسل طلب يحمل رقم البطاقة البنكية الخاصة به وكذا حسابه البنكي بالبريد العادي أو عن طريق الهاتف ومنها يحصل على شهادة معرف (Identifiant) من طرف الشركة، ولتأمين خصوصية المعلومات البنكية تستعمل حروف وأرقام سرية لأن كل المعلومات والبيانات تنتقل عبر شبكة الأنترنت⁽²⁾.

ترتكز عملية النظام الافتراضي على ثلاث عمليات تتم بين العميل والتاجر والشركة الوسيطة، حيث هناك عمليات تتم على الترتيب، حيث يستقبل التاجر الرقم الخاص بالتعريف الشخصي للعميل، وبعد تأكد التاجر من القيمة الحسابية الكافية الموجودة لدى البنك الوسيط يقوم بتحويل المعلومات المتعلقة بالصفحة موثقة بالرقم الخاص بالتعريف الشخصي الخاص به وكذا الخاص بالعميل، ومن أجل أن تتحقق الشركة من عملية التسوية تقوم بإرسال رسالة إلكترونية ليتطابق العميل مع هويته⁽³⁾.

بعد قبول ورضا العميل يتم تحويل كل المعلومات الخاصة بالعميل والتاجر عن طريق أحد البنوك التقليدية، والتي عبرها تتم عملية التنفيذ بتحويل النقود من حساب العميل

(1)- محمود محمد أبو فرة، الخدمات البنكية الإلكترونية عبر الإنترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2009، ص 74.

(2) فاروق محمد الأباصيري، عقد الاشتراك في قواعد المعلومات عبر شبكة الانترنت، دار الجامعة الجديدة القانونية، الإسكندرية، مصر، 2002، ص 103.

(3)- انظر: علي أحمد نعمان، الحماية التقنية للتجارة الإلكترونية، مجلة القانون، عدد 1، مطبعة وراقة وطنية، المغرب، 2011، ص 20.

إلى الشركة الوسيطة، فتقوم هذه الأخيرة بتحويل النقود للتاجر وإعلامه بتنفيذ الوفاء لتتم عملية تنفيذ الالتزام مع العميل بعد إخطار التاجر قبلها بعملية التنفيذ

الفرع الثاني: نظام (Kleline)

يعتمد هذا النظام على متابعة المشاريع الخاصة بتطوير مشاريع البرمجيات مفتوحة المصدر، أي يمكن لأي كان أن يقوم بتعديل تقنية المشروع باعتبار أنها مصممة للجميع حتى يسمح للابتكارات والإبداعات الفنية أن تتقدم وتتطور بسرعة مثل إضافة أشياء جديدة أكثر تطوراً وسرعة، ويعد هذا النظام برنامج وفاء آمن يساهم في حماية الحساب الإلكتروني الشخصي، ويتلقى التاجر من العميل طلب مفاده الحصول على سلعة معينة بغرض شرائها، ويتوجه التاجر إلى الشركة الوسيطة ببطاقة الوفاء الإلكتروني، ومنه تقوم هذه الأخيرة بالتوجه إلى العميل وتحويله بطاقة الوفاء⁽¹⁾

يقوم العميل بقبول بطاقة الوفاء وصدور الرضا منه تمنح (Kleline) قسيمة صندوق (Bon de caisse)⁽²⁾ للتاجر، وذلك لاستكمال إجراءات عملية الوفاء، ومن أهم الخصائص التي يختص بها (نظام Kleline) هي تحقيق الحماية الكافية والأمان في إجراءات الوفاء بواسطة حاسوب خاص بالعملية لتحقيق إمكانية فعلية تواجد التاجر المسجل سلفاً بالشركة، وقد لعب وسيط الوفاء الإلكتروني دوراً فعالاً في التقليل من عراقيل وصعوبات الوفاء الإلكتروني؛ لأنه لا يمكن أن يتدخل الإرهاب الإلكتروني بهوية مجهولة، فالوسيط بين المتعاقدين يمنع ذلك ويوفر أمن وحماية بين العملاء والموردين.

المطلب الثاني: حافظة النقود الإلكترونية والافتراضية

تعتبر كل الإصدارات الرقمية لبطاقات الوفاء الائتمانية مخصصة للخصم المباشر بمثابة محفظة رقمية، حيث يتم ذلك مع المستخدم عن طريق تخزينها بالهاتف الذكي في تطبيق خاص بها والذي يحمل على الهاتف الذكي قصد استعماله وتوظيف هذه العملية في

(1) علي أحمد نعمان، المرجع السابق، ص 21.

(2) يمكن القول: أنها ودائع لأجل دين والقوائم النقدية هي حلول مصممة خصيصاً يقدمها بعض البنوك مثل: Société Générale Algérie، وهذا حتى تتمكن من تعزيز رأس المال الخاص بك على المدى القصير والمتوسط، والوديعة المخصصة للاستثمار عند الاكتتاب مسبقاً تعرف شروط تثبيته وكل عوائده، حيث يعد استثمار مالي بالدينار الجزائري كدين، كما ينفذ عن طريق شخص طبيعى أو معنوي، ويتم تسجيله على حامل أو مجهول.

مختلف العمليات المصرفية الرئيسية، وتشتمل فكرة النقود الإلكترونية على توافيق رقمية وبروتوكولات مطابقة لمختلف العملات الكلاسيكية التقليدية، والتي تسمح للرسالة الإلكترونية أن تتوافق فعلياً معها⁽¹⁾.

ظهرت العملة الافتراضية في سنة 2008، وقد أشار إليها الباحث "ساتوشي ناكاموتو"، حيث تم طرحها للتداول سنة 2009 حيث تم استعمالها في العالم الرقمي الافتراضي على شكل عملة رقمية غير ملموسة في الواقع المادي، وبعدها انتشرت في أغلب دول العالم باعتبارها عملة دفع إلكتروني عابر للحدود الجغرافية للدول⁽²⁾.

تعد العملة الافتراضية من أبرز الأنواع الجديدة التي تنتمي إلى النقود الرقمية باعتبار أنها تنحصر في الفضاء الرقمي، حيث تنتج في بيئة رقمية بإعداد برامج في الحاسوب مخصصة لها من حيث دورها تخزين في مجموعة من المحافظ الإلكترونية، ويشترط في الولوج إليها الاتصال بشبكة الأنترنت عبر هواتف ذكية أو حاسوب، وقد عرفها المشرع الجزائري في المادة 117 من قانون المالية 2008 أنها: "تلك التي يستعملها مستخدمو الأنترنت عبر شبكة الأنترنت، وهي تتميز بغياب الدعامة المادية كالقطع والأوراق النقدية وعمليات الدفع بالصك أو البطاقة البنكية".

يتضح من خلال المادة 117 من قانون المالية لسنة 2008 أن كل العملات الافتراضية تعتبر رقمية، أما النقود الرقمية فليست في زمرة الافتراضية لأن النقود الإلكترونية كذلك نقود رقمية، وكون أنها من الأرصدة الورقية والتي تم تحميلها إلكترونياً بطريقة ممغنطة على شكل بطاقة بلاستيكية فإنها ليست مشابهة للنقود الافتراضية تقوم بإصدارها إما بنوك افتراضية أو بنوك رقمية.

الفرع الأول: النقود الإلكترونية (Monnaie électronique)

إن أبرز خصوصية للنقود الإلكترونية هي كونها وسيلة تتميز بالحدثة تتعلق بالوفاء الإلكتروني وكذا الأداء المالي، وتعتبر ابتكاراً يوفي بالغرض في البيئة الرقمية، كما أنه نتاج التكنولوجيات المتطورة في جانب العمليات المصرفية والمالية⁽³⁾، وتمثل تقنية النقود

(1) إبراهيم بخي، المرجع السابق ص 72.

(2) أحمد محمد عصام الدين، "ماذا تعرف عن عملة البيتكوين Bitcoin"، مجلة المصرفي، إدارة البحوث والتنمية، عدد 73، سبتمبر 2014، ص ص 50-53، ص 51.

(3) بهلولي فاتح، المرجع السابق، ص 313.

الإلكترونية في عملية الجمع بين عدة وحدات لتوحيد القيمة بعيدا عن القيمة المالية في البنك وحساباته، ونتج عن ذلك اتجاهين، الأول هو ما يسمى بحافظة النقود الإلكترونية "PME"، والثاني يطلق عليه اسم حافظة النقود الافتراضية "PMV" حافظة النقود الإلكترونية يسجل رصيدها المالي في بطاقة بعد شحنه من قبل برصيد مالي، أما حافظة النقود الافتراضية يستعمل فيها حاسوب متصل بالشبكة يتم شحن رصيد مالي بقرض خاص به، كما تتنوع النقود الإلكترونية في أشكال مختلفة، النقود الإلكترونية البرمجية، المحفظة الإلكترونية، الشبكات الإلكترونية، والبطاقات المصرفية

أولا: النقود الإلكترونية البرمجية: تعد النقود الإلكترونية البرمجية من أشهر الأنواع المعتمدة في برمجيات معينة قصد استغلال النقود الإلكترونية واستغلالها في البيئة الرقمية للقيام بشراء سلعة أو بضاعة ما، وتظهر المحفظة الإلكترونية في شكل بطاقة ذكية تسمح لنا بوضعها في الكمبيوتر الشخصي، أو قد تكون في شكل قرص مرن يمكن وضعه في الكمبيوتر الشخصي في الفتحة الخاصة بالقرص، وبالتالي تتم عملية تحويل القيمة المالية من هذا القرض وإليه عبر شبكة الأنترنت المتاحة كوسيط إلكتروني ليحصل المشتري على النقود الإلكترونية⁽¹⁾.

ثانيا: المحفظة الإلكترونية: يقصد بالمحفظة الإلكترونية أو المحفظة الرقمية كما أشرنا إليها سابقا عملية تتم بتنظيم جميع الحركات المالية ضمن تطبيق رقمي معين، حيث تتم بشكل مشفر تتضمن المحفظة كل التفاصيل والبيانات المتعلقة بهذه البطاقة، وتدعى نقود الشبكة أو الأنترنت، حيث يتم تداولها بين المتعاملين بعد حفظها عبر وسيلة رقمية فتقبل باعتبارها وسيلة للدفع بغض النظر عن من قام بإصدارها⁽²⁾.

ثالثا: الشيكات الإلكترونية: لم يخصص المشرع الجزائري أحكام أو نصوص متعلقة بالشيك الإلكتروني بصفة خاصة مثل الأوراق التجارية الإلكترونية، ويعود هذا إلى عدم التعامل بالشيك الإلكتروني لأنه حديث العهد في المعاملات الإلكترونية المحلية مثل وسائل الدفع، واتخذ المشرع الجزائري تجربة الأوراق التجارية على أرض الواقع على ضوء أحكام

(1) دانون سمير، العقود الإلكترونية في إطار تنظيم التجارة الإلكترونية، المؤسسة الحديثة للكتاب، لبنان، 2012، ص175.

(2) بهلولي فاتح، النظام القانوني للتجارة الإلكترونية في ظل التشريع الجزائري أطروحة لنيل درجة الدكتوراه في العلوم، تخصص قانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 2017، ص215.

القواعد التقليدية العامة، وقد حث عليها التشريع في القانون 03-15 الموافق للأمر 03-11 المتعلق بالنقد والقرض، ويعد أول تشريع جزائري تطرق في القطاع المصرفي قصد التعامل الإلكتروني، أما الأمر 05-06 الصادر بتاريخ 23 أوت 2005 المتعلق بمكافحة التهريب، حيث انتهج المشرع الجزائري كل الأمور التي تتعلق بالإجراءات والتدابير الوقائية لمواجهة ومكافحة التهريب وعبر عنه صراحة في المادة الثالثة منه بالدفع الإلكتروني ويعد الشيك الإلكتروني مساويا لمختلف الشيكات التقليدية الورقية، يعرف بأنه رسالة إلكترونية تتميز بالأمان والتوثيق ترسل على شكل وثيقة مخصصة للدفع تتضمن التوقيع الرقمي للمرسل الذي صدر عنه الشيك إلى مستلم الشيك⁽¹⁾.

ثالثا: البطاقة المصرفية: هي في الغالب بطاقة بلاستيكية يقوم البنك بإصدارها لصالح عملائه، وهي تمنح العديد من الخدمات لفائدة العميل من أجل الوصول إلى حساب مصرفي معين، وتسمى كذلك ببطاقات المعاملات المالية يستطيع حاملها أن يحصل على خدمات أو سلع أو نقود، وهي نوعان: البطاقة المصرفية الائتمانية التي تسمح لحاملها بأخذ قرض ائتماني، والبطاقة المصرفية غير الائتمانية التي تتميز بجانب من جوانب التقييد، وهي نادرة الانتشار في تطبيقات البيئة الإلكترونية.

الفرع الثاني: النقود الافتراضية

يقوم الإرهاب الإلكتروني باختراق البيانات والمعلومات المتوفرة على شبكة الأنترنت، وتساهم هذه التقنية في مواجهة وتجنب اختراق المعطيات الموجودة على الشبكة، ومن أهداف هذه التقنية هي وضع وحدات القيمة الإلكترونية ذات مستقلة لتستطيع أن تسيطر على وضعية استعمالها وتوظيف أهداف غير مشروعة في ذلك، فالاحتياط هو قفل أو غلق الرموز الرقمية الإلكترونية لنتمكن من نقل ذلك القيمة الإلكترونية من محفظة إلى محفظة إلكترونية أخرى، وننتهي بتحويل النقود من إلكترونية إلى رقمية، ومن عوامل انتشار العملة الافتراضية هي:

أولاً: لا مركزية العملة الافتراضية: من أبرز ما تتميز به العملة الافتراضية هي عملية دفع لا مركزية فهي نظام دفع عابر للحدود ليس له أي انتماء مركزي، ومن جهة أخرى تستبعد فكرة التزوير وإحداث بعض التغييرات عليها، وتعمل اللامركزية على تفادي تأثير

(1) إبراهيم بخي، المرجع السابق، ص 73.

العملة الافتراضية الطوارئ والتغيرات ذات البعد السياسي في دول العالم⁽¹⁾.

ثانيا: ديناميكية التعامل بالعملة الافتراضية: تكمن المعاملات المالية هنا في تسوية مالية بطريقة مباشرة دون اللجوء إلى الوسيط حتى تخفف من قيمة الأعباء الناتجة عن الوفاء بذلك⁽²⁾، ويستطيع المتعامل أن يوفر المال والوقت والجهد، وبإمكانه إرسال أو استقبال أي قيمة مالية عبر العالم.

ثالثا: العملة الافتراضية وسيلة استثمار مربحة: إن ما يميز العملة الافتراضية هو أنها تتصف بالندرة⁽³⁾ لذلك فإن أسعارها مرتفعة جدا نظرا لانخفاض أسعار التكاليف اللازمة مقابل المعاملات المالية في شكل العملة الافتراضية، وبذلك يرفع من الربح التجاري الذي يتحقق من خلال هذه المعادلة.

رابعا: ضمان سرية التعامل بالعملة الافتراضية: يعود ذلك إلى أن التعامل في أغلب العمليات التي تتم فيها المعاملات المالية عبر وسيط البيئة الرقمية بواسطة العملة الافتراضية تخضع لسرية تامة من خلال عدم التعرف عن هوية الأشخاص الذين يتعاملون بالحقل الإلكتروني، بالإضافة إلى خصوصية النظام البنكي اللامركزي⁽⁴⁾

المبحث الثاني: حماية المواقع الخاصة بالأنترنت

تتدخل عدة عوامل في حماية المواقع الخاصة بالأنترنت، ولمواجهة أخطار القرصنة واختراق المعلومات والبيانات توجد وسائل كثيرة تعمل على تأمين المواقع الإلكترونية، وتقدم أحسن شركات العالم حماية فعالة بمعايير ممتازة وجودة فائقة، تتصدى لبعض البرامج التي تزرع فيروسات قد تشكل خطورة وضرر كبير، لذلك من أهم وسائل حماية البيانات الحساسة الموجودة على الشبكة والتصدي لها هي استخدام فنيات وتقنيات التعمية أو التشفير المتطورة، وكذا جانب آخر يتمثل في أخذ الاحتياطات اللازمة في نسخ المواقع

(1) حمد زيدان، أسباب تدفعك لشراء بتكوين وأخرى تحذرك من الاتجار بها، 4 جانفي 2008، تم الاطلاع عليه يوم 03 سبتمبر 2024 الساعة 23:15 متوفر على الرابط <http://bit.ly/38+lbQo>

(2) حسن محمد مصطفى، دور عملة البيتكوين في تمويل وتنظيم الجماعات الإرهابية، صحيفة حفريات، مركز دال للإنتاج والأبحاث والإنتاج الإعلامي، مصر، 2017، تم الاطلاع عليه يوم 05 سبتمبر 2024، الساعة 00:28 ص 13 متوفر على الرابط: <http://bit.ly/38ttduD>

(3) راجع في ذلك: نور الدين صويلحي، أثر البيتكوين والعملات الافتراضية على استقرار النظام النقدي العالمي، مجلة آفاق علمية، المركز الجامعي بتمنراست، الجزائر، المجلد 10، عدد 2، سنة 2018، ص ص 219-239، ص 227

(4) انظر في هذا المعنى: حسن محمد مصطفى، المرجع السابق، ص 11.

الإلكترونية المهمة (المطلب الأول)، وللحفاظ على سرية تداول المعلومات وأمنها يستعمل تشفير وفك تشفير البيانات والمعلومات⁽¹⁾.

كما يلعب الجدار الناري كوسيلة هامة لحماية مضمون البيانات فهو نظام آمن لا يكلف كثيرا لمواجهة الأخطار والهجمات الخبيثة، حيث يتم التحكم عن طريق توظيف شبكة الأنترنت ولا يحتاج إلى استخدام برامج معينة، ويعد مفهوم الجدار الناري وسيلة مميزة في حماية المواقع الإلكترونية وظيفتها حماية الشبكات الخاصة من الولوج إليها ومن جهة أخرى تصدّ ولا تسمح بدخول الشبكة غير المشروع فهي تؤمن وحدة إرسال واستقبال المعلومات والتحكم فيها (المطلب الثاني)⁽²⁾.

المطلب الأول: نظام التشفير كوسيلة لحماية سرية المعلومات

إن التشفير يعرف كآلية ووسيلة تؤمن وتحمي كل المعلومات القيمة كالصور والوثائق والمعاملات الإلكترونية عبر شبكة الأنترنت، وذلك باستخدام شفرة وهي عملية رياضية لمنع الأشخاص من الولوج إلى البيانات أو محاولة تغيير محتواها، وتعد عملية تركيب وتشفير علم يقوم بكسر الاتصالات الآمنة، ولذلك لا يسمح لأي شخص من قراءة محتوى ومضمون الرسالة الإلكترونية ماعدا الذي ترسل له البيانات والمعلومات الإلكترونية، ولذلك يجب أن تخضع بيانات التعاقد ومعلوماته إلى إجراءات وقائية محكمة عند تداولها حتى تكون في حماية تامة، وتكون آمنة من التلاعب والعبث بمحتواها⁽³⁾، ولا يسمح التشفير لغير المعنيين من التقاط البيانات والمعلومات والرسائل محاولا بذلك منع وصولها أو على الأقل لا تصل مقروءة ومفهومة وتكون مشوهة الحروف، وبالتالي يتطلب الأمر حماية فعالة تسمح بوصولها بالصورة المقبولة لمستقبل البيانات المرسل⁽⁴⁾.

(1) راجع في ذلك: عمر خالد زريقات، عقد التجارة الإلكترونية (عقد البيع عبر الأنترنت- دراسة تحليلية)، دار حامد للنشر والتوزيع، عمان، الأردن، 2007، ص 269.

(2) يمكن القول: أن الجدار الناري هو إجراءات وقائية آمنة تمثل أنظمة محكمة ذات وظيفة آمنة ترتبط بين المؤسسة وشبكة الأنترنت، ودورها الأساسي هو أنها تتحكم كل العمليات التي تمر عبر الشبكة والخروج منها بالمرور من الجدار الناري حتى يستطيع أن يتعرف على المتطفلين ومنعهم من الدخول.

(3) حليتيتم سراح، حماية المعاملات القانونية على تقنية التشفير الإلكتروني، ضمن فعاليات الملتقى الوطني حول الإطار القانوني للتوقيع والتصديق الإلكترونيين في الجزائر، يومي 12 و 13 جانفي 2016، بجامعة محمد الشريف مساعدي، سوق أهراس، ص 1.

(4) عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، دار الفكر الجامعي، مصر، 2004، ص 3.

يعرف التشفير بتحويل المعلومات والبيانات المقروءة والمفهومة إلى رموز ليس لها معنى ولا يسمح فقط للأشخاص المرخص لهم من الوصول إلى المعلومات والبيانات وفهم مضمونها، حيث مع نقل المعلومات المتمثلة في التوقيع في الشكل الإلكتروني وكذا حركة الأموال المتداولة عبر الشبكة بتحويل نصوص مفهومة إلى نصوص مشفرة وذلك لحمايتها من القرصنة الإلكترونية⁽¹⁾.

ينتشر خطر استخدام التكنولوجيا من جانب الإرهاب والتطرف وخصوصا بالنظر إلى النقلة التي عرفتها المعلوماتية في مجال الذكاء الاصطناعي، وهو نظام حاسوبي بإمكانه أن يصل إلى تقنيات تتجاوز الجانب الفني عبر الشبكة إلى أجهزة مسيرة كالروبوتات والطائرات المسيرة، والبرمجيات الضارة والهجمات التي تحجب الخدمة عن طريق الهجوم على مواقع معينة، وبذلك نلجأ إلى تشفير الرسائل الإلكترونية إما بارتباطها بالتجارة الإلكترونية أو غير ذلك باستعمال رموز وإشارات لا توجد إمكانية معرفة تفكيك وقراءة وفهم المعلومة إلا بفك التشفير⁽²⁾، فتأمين البيانات والرسائل الإلكترونية ومحتوى المعلومات يجب أن يخضع لعملية التشفير لمنح حماية كافية لمحتوى الرسالة الإلكترونية، وهناك نظامين في استخدام تقنية التشفير من الناحية الفنية، فيعرف الأول بالنظام السيمتري أو المتماثل، أما النظام الثاني فهو النظام أسيمتري اللامتماثل، إضافة إلى نظام المعاملات الإلكترونية الآمنة، ونظام التأمين، وتتناول كل هذا في الفرع الأول (التشفير المتماثل والتشفير اللامتماثل)، والفرع الثاني (نظام المعاملات الإلكترونية الآمنة، ونظام التأمين)

الفرع الأول: نظام التشفير المتماثل ونظام التشفير اللامتماثل

التشفير المتماثل آلية تقنية للتشفير حيث يستعمل مفتاح سري قصد تشفير رسالة ما أو وضع عملية رياضية للتعمية وفك تشفير هذه الرسالة، ويستعمل نفس المفتاح في العمليتين، التشفير وفك التشفير ولذلك يسمى بالمفتاح المتناظر، ويتطلب الأمر كل ذلك، ويعد التشفير نظام يحافظ على حماية وسلامة التبادل الإلكتروني ويحافظ على السرية⁽³⁾ تمنح هذه التقنية حماية كبيرة لضمان السلامة والأمن داخل الشبكة، أما التشفير

(1) هدى حامد قشقوق، الحماية الجنائية للتجارة الإلكترونية عبر الأنترنت، دار النهضة العربية، مصر، 2000 ص 61.

(2) يمينة حوحو، عقد البيع الإلكتروني في القانون الجزائري، دار بلقيس، الجزائر، 2016، ص 185.

(3) عبد الفتاح بيومي حجازي، المرجع السابق، ص 211.

اللامتناثل فيستعمل فيه مفتاح للتشفير ومفتاح آخر لفك التشفير، ولذلك تدعى هذه العملية التشفير بالمفتاح اللامتناظر، ومعنى ذلك أن التشفير المتناظر يستخدم فيه المفتاح العام في عملية التشفير وكذا في عملية فك التشفير، أما التشفير اللامتناظر فيستخدم في عملية التشفير مفتاح عام، ويستخدم مفتاح خاص لعملية فك التشفير.

أولاً: التشفير المتماثل **La cryptographie symétrique**: وهو التشفير الذي يقوم به صاحب الرسالة ويستخدم في ذلك المفتاح العام نفسه من أجل إنشاء التوقيع بالشكل الإلكتروني، وعندما يتواصل مع المرسل إليه ويتم الاتفاق على كلمة السر التي تكون بينهما ويقوم بفك التشفير (التعمية)⁽¹⁾، ومضمون اتفاق طرفي الرسالة في عملية التشفير هو التغيير من كلمة المرور إلى عدد ثنائي مع زيادة أشكال ورموز أخرى لزيادتها⁽²⁾، وبذلك يتشكل عدد ثنائي والذي يصبح مفتاح تشفير هذه الرسالة، وهو ناتج مفتاح التشفير، وكلمة السر الناتجة عن تغيير أرقام أو حروف أو رموز إلى عدد ثنائي بعد زيادة حروف أخرى إليها، أثناء استقبال الرسالة يستعمل مستقبلها نفس كلمة المرور قصد تفكيك عبارة النص الذي كان مشفراً، حيث يتشكل المفتاح الثنائي بعد ترجمة كلمة المرور عن طريق برمجيات التشفير، وهذه الفنيات توظف في استعمالها مجموعة من الحروف أو الأرقام المعقدة حتى يستحيل العبث بها وتزويرها⁽³⁾.

ثانياً: التشفير اللامتناثل: **La cryptographie asymétrique**: التشفير اللامتناثل هو ما يسمى (الهندسة العكسية)، حيث يستعمل في ذلك مفتاحان، المفتاح الأول عام، والثاني مفتاح خاص، وكل منهما له علاقة رياضية معقدة يعرفها فقط صاحب المفتاح نفسه⁽⁴⁾، ويمثل التشفير اللامتناثل طريقتين مختلفتين لعملية تشفير محتوى الرسالة وعملية فك التشفير أثناء استقبال الرسالة يستخدم فيها المفتاح العام والمفتاح الخاص⁽⁵⁾، والمفتاح الخاص هو ملك لشخص واحد له وظيفة لتشفير الرسالة وفك شفرتها، والمفتاح العام يفك شفرة الرسالة التي قام بتشفيرها المفتاح الخاص، ومن جهة أخرى لا

(1) حليتييم سراح، المرجع السابق، ص 4.

(2) بلقاسم عبد الله، المحررات الالكترونية وسيلة لإثبات العقد الإلكتروني (دراسة مقارنة)، مذكرة ماجستير في القانون، فرع القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة تيزي وزو، 2013، ص 134.

(3) عبد الفتاح بيومي حجازي، المرجع السابق، ص 211.

(4) عبد الفتاح بيومي حجازي، المرجع نفسه ص 212.

(5) يمينة حوحو، المرجع السابق، ص 188.

يمكن للمفتاح العام أن يفك الرسالة التي شفرها المفتاح الخاص، ولا يمكن للمفتاح العام أن يفك رسالة مشفرة بالمفتاح العام⁽¹⁾، وهناك شروط قانونية أساسية تتمثل في ضوابط وقواعد وأسس مسموحة من الناحية القانونية تتمثل في تشفير البيانات والمعلومات التي تدون عبر وسائط إلكترونية معدة لذلك، حيث تتوفر الشروط الأساسية التي حددها المشرع يتم الاعتراف القانوني للتشفير كوسيلة لتحرير البيانات مع إلزامية وضرورة احترام السرية والأمان والثقة لهذه البيانات⁽²⁾.

الفرع الثاني: نظام المعاملات الإلكترونية الآمنة (Set) ونظام التأمين (SSL):

يقصد بها بروتوكول اتصال قامت باستعماله إحدى المواقع التجارية الإلكترونية حتى تضمن سلامة وأمن مختلف المعاملات المالية وكل ما يتعلق بالدفع الخاص ببطاقة الائتمان عبر شبكة الأنترنت، وبذلك ظهر ما يسمى بروتوكول المعاملات الإلكترونية الآمنة والذي يختصر بـ (Set) الذي تم تطويره بداية من سنة 1996، حيث قامت اغلب الشركات العالمية المرتبطة بخدمات المعاملات المالية الإلكترونية مثل ماستر كارت وفيزا بدعم مباشر لهذا البروتوكول، ومنه يتم الحصول على شهادات رقمية مشفرة لجميع الزبائن عند القيام بعملية الشراء والتي تحتاج إلى الدفع الإلكتروني عبر الشبكة سواء عن طريق الحسابات البنكية أو بطاقة الائتمان وبالتالي هذا البروتوكول يتيح للتجار التأكد من المعلومات الصحيحة لحماية المعلومات المرتبطة خصيصاً بالعملاء، أما نظام التأمين فيعرف بكونه شهادة رقمية تصادق على الهوية التعريفية لموقع الويب وتسمح للقيام بالاتصال المشفر الذي يتوجه إلى مأخذ توصيل آمنة، حيث يعرف هذا البروتوكول ببروتوكول أمان يربط بين تشفير مستعرض الويب وخادم الويب، كما يمنع المتطفلين من قراءة وفهم البيانات والمعلومات المنقولة بين نظامين أو التعديل فيها، وتحافظ خصوصاً على أمن وسلامة اتصال شبكة الأنترنت.

أولاً: نظام المعاملات الإلكترونية الآمنة (Set)⁽³⁾: يهدف هذا البروتوكول خصوصاً إلى تأمين الوفاء والمعاملات المالية بمناسبة العمل التجاري، فهو نظام يتميز عن غيره من الأنظمة

(1) حليتيتم سراح، المرجع السابق، ص 4.

(2) بلقاسم عبد الله، المرجع السابق، ص 135.

(3) يمكن القول: أن المعاملات الإلكترونية الآمنة اختصرت فيما يسمى ببروتوكول اتصال تم استعماله في مواقع خاصة بالتجارة الإلكترونية حتى تسمح بالحفاظ على أمن وسلامة وثقة المعاملات المالية، وكذلك كل دفع خاص ببطاقة ائتمان عبر شبكة الأنترنت، فهو يسمح للأنظمة من التأكد والتحقق من الهوية التعريفية ومنه ينشأ اتصال شبكي يكون مشفر، تم إنشاء هذا البروتوكول أول مرة سنة 1996 للاطلاع عليه عبر الرابط: <https://aws.amazon.com>

التأمينية الأخرى، حيث انطلاقاً من الطلب الذي تتضمنه المعلومات المشفرة فإنه يحافظ على تأمين وسلامة سرية الطلبية المتعلقة بالشراء، إضافة إلى أنه يشتمل على البيانات المتعلقة بخصوصية عملية الوفاء، كما تخصص بصمة ورقية خاصة بالطلب تسمح بمطابقة الطلب الذي يستقبله التاجر أو صاحب المشروع لنفس طلب الشراء الذي تم إرساله.

ثانياً: نظام التأمين (SSL): إن شهادة نظام التأمين تجعل مستعملي المواقع الإلكترونية في أمان وثقة تامة، حيث باستخدام المواقع يتم تثبيت الشهادات من قبل الشركات لتصبح مؤمنة تماماً⁽¹⁾، ويقوم بروتوكول هذا النظام بالتدخل المباشر للتصدي لجميع الاتصالات الموجودة في الشبكة وتشفيرها في مختلف البرامج الخاصة بالتصفح وكل النوافذ المتعلقة بالشبكة المعلوماتية، والمقر الرسمي للمعلومات الموجودة بالمواقع على الشبكة، وبالتالي يؤمن المعلومات عند انتقالها ويغلق الباب أمام وقوعها في حوزة أشخاص غير معنيين، وفي نهاية العملية يمنح مستقبل المعلومات الثقة والطمأنينة في سلامة المعلومات والبيانات المتعلقة بهم التي وصلت ولم تتح إلا للمعنيين من مؤسسة أو منشأ أو تاجر، والمتضمنة معلومات البطاقات البنكية المؤمنة.

المطلب الثاني: الجدران النارية كوسيلة لحماية المحتوى

يمكن الجدار الناري أو ما يسمى بجدار الحماية الذي يراقب حركة الشبكة من صادر ووارد على الحاسوب الخاص انطلاقاً إلى الأسس الموجودة وكذا بعض الأسس التي نقوم بتحديددها، حيث تتم بذلك إمكانية فتح المجال أمام الشبكة الشخصية أو رفض ذلك، فيتصدى لهجمات قادمة من أجهزة أخرى، ويستطيع أن يمنع ويوقف خدمات معينة قد تأتي بتهديدات ويؤمنها ويحميها من ذلك، ويقضي على التطفل المحتمل⁽²⁾.

يقوم الجدار الناري بحماية الشبكات الخاصة، وباستخدام الأجهزة السمعية البصرية يبث لمضيفين عن طريق مؤتمرات فيديو، ومن أبرز إيجابيات الجدار الناري أنه يقوم بتسجيل جميع حركات المعلومات التي تمر، وكذلك تسجيل وتدوين كل واقعة استعملت كون أن كل الرسائل تمر عن طريقه أثناء ولوجها الشبكة أو الخروج منها، وتعمل على الحد من الشبكة بفضل حمايتها المحكمة للمعلومات.

(1) قانون رقم 15 - 04 مؤرخ في 11 ربيع الثاني 1436هـ/الموافق ل 1 فبراير 2015 يحدد القوانين العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج ر، عدد رقم 6 صادر في 10 فبراير 2015.

(2) علي أحمد نعمان، المرجع السابق، ص 39.

الفرع الأول: تعريف الجدار الناري

يقصد به ذلك النظام الذي يعمل على توفير حماية وأمان للشبكة، وانطلاقاً من معطيات وقواعد وضعها المستخدم وبتحسين البيانات التي ترسل وتستقبل عن طريق الشبكة، والتي تهدف إلى القضاء أو التقليل من وجود الاتصالات الشبكية غير المرغوب فيها، وتوفير الجدار الناري الذي يسمح للاتصالات الخاضعة للقانون بالانتقال بكامل

الحرية، وبفضل الحماية الكافية يتم منع أي هجوم محتمل من المساس والعبث بالخدمة بطرق غير مشروعة وغير سوية⁽¹⁾.

أولاً: مزاي الجداري الناري: كما أسلفنا الذكر فإن البرامج تسمح لأي مستخدم أن

يدخل الشبكة، ومع توفر الجدار الناري فإن أي استخدام غير مشروع سوف يصده الجدار الناري، ومن أهم المزايا التي يتمتع بها الجدار الناري أنه يقف في مواجهة كل من يريد أن يعيث بمعلومات وبيانات الشبكة والتقليل من الأخطار المحتملة الحدوث، وكذلك مراقبة كل المستجدات التي تدخل وتخرج من الشبكة وذلك بتسجيلها الأوامر والرسائل قصد معرفة كل تفاصيل الاستعمال، وتدوين كل الحركات التي تمر بها المعلومات داخل الشبكة.

ثانياً: عيوب الجدار الناري: يتميز الجدار الناري بالعديد من العيوب منها:

أ- التكلفة: إن أنواع الجدران النارية تعتمد في بعض الاستثمارات بصفة عامة، لأنه بالنسبة للجدران المخصصة لحماية الأجهزة المستعملة تفوق بكثير تكلفة حماية البرامج، بالإضافة إلى أن برامج الأجهزة تحتاج صيانة مستمرة وتثبيت، وكذا مبالغ مالية إضافية مع تكلفة التكوين الذي يحتاج إلى خبير متخصص في إدارة وتسيير المعلوماتية.

ب: تقييد المستخدم: حماية الجدران النارية لا تسمح للولوج إلى نظام المستخدم بالشبكة إلا من كان مصرح له بذلك مما تنعكس سلباً على المؤسسات الكبيرة والتي تؤثر على الإنتاج الكلي للشركة.

ج: الأداء: تعتبر تكلفة ذاكرة الوصول العشوائي والمعالجة أساسيات تحديد ما يؤديه الحاسوب لأنه تعتمد في ذلك على موارد الحاسوب.

(1) راجع في ذلك: قانون رقم 04-09 مؤرخ في 2009/08/05 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر، عدد 47، صادرة بتاريخ 2009/08/16.

د: هجمات البرمجيات الخبيثة والعمليات المعقدة: الأول يوصي بتثبيت برمجيات تقوم بمواجهة البرامج الضارة رغم الحماية، والتي تملك القدرة على التصدي لكل نوع رئيسي من أحصنة طروادة،

أما بخصوص العمليات المعقدة يجب التصدي للمتطفلين رغم أن جدار الحماية أصبح من السهل أن يقوم بصيانة الشركات الصغيرة إلا أنه يحتاج إلى حماية منفصلة⁽¹⁾.

الفرع الثاني: أنواع الجدار الناري

يتكون الجدار الناري للشبكة من ثلاثة أنواع رئيسية هي: ترشيح الرزم (packet filtering)، أو عديمة الحالة (stateless)، ذات الحالة (stateful)، وطبقة التطبيقات

أولاً: ترشيح الرزم: وهي عبارة عن نوع خاص من الجدار الناري عديم الحالة، وتقوم بتوزيع جميع الرزم، وعليه لا تستطيع أن تتصل، وتعمل على تمكين مرور الرزم انطلاقاً على تجميع مختلف الرزم بصورة فردية.

ثانياً: الجدران ذات الحالة: وتتميز عن الجدران عديمة الحالة بمرونة أكثر باعتبار أنه باستطاعتها التعيين والتمكين، ومعرفة حالة الاتصال بالرزم، وتقوم على إمكانية التقريب بين الرزم المتجمعة حتى تتمكن من تحديد حالة الاتصال لما يسبق.

خاتمة:

ختاماً لموضوعنا هذا وعلى ضوء ما تعيشه تطورات التجارة الإلكترونية في البلدان النامية خصوصاً، وفي دول العالم عموماً، والذي تمثل نقص كبير لدى عدد الأشخاص الذين يستعملون شبكة الأنترنت في إبرام مختلف المعاملات التجارية، ويعود هذا للكثير من الأسباب والعوامل من أبرزها البنية التحتية للتجارة عبر الأنترنت، ونقص ثقافة التعامل الرقمي والإلكتروني، وانتشار الأمية بصفة عامة.

إن التطور التكنولوجي، والتقدم في مجال المعلوماتية نتج عنه سن قواعد تهدف إلى

انظر: أحمد عباس، ووردبريس بالعربية، شرح الجدار الناري (Firewall) وأنواعه وتفعيله على موقعك للحصول على حماية كاملة، بالنظر إلى وهو نوع Firewall الذي سبقهم كلهم، كما يتميز بالسرعة والنوعية في التركيز على الاتصال وأحسن مركز يعتمد على جانب خارجي IP والتي تتصل بصور المعلومات والوصول إليه، متوفر على الموقع:

<https://www.wpar.net>

حماية أمن المستهلك، لكن لم تكن كافية باعتبار أنها حماية خاصة أفرزت جانب المعالجة لارتباطها بخصوصيات معينة، ومن جهة أخرى تحتاج إلى الاهتمام المطلق بالحماية الوقائية، وهو ما نتج عنه الذهاب إلى توفير الحماية اللازمة المرتبطة بطبيعة تقنية في بيئة رقمية تزرع الطمأنينة والثقة في نفسية المستخدم بالإضافة إلى أن الكثير من التحديات والمصاعب والمخاطر تواجه البيئة الرقمية لأن نوعية المعلومة هي التي تحدد درجة الحماية اللازمة لذلك، وبالتالي تنطلق إجراءات الحماية من الاحتياجات اللازمة، والتي تهتم بحماية المعاملات المالية الإلكترونية عبر الشبكة، وكذا حماية المواقع المرتبطة بالإنترنت.

إن آخر ما خرجنا به من نتائج في بحثنا هذا تمثل أساساً في فرض حماية قانونية تمنح حماية إلكترونية خاصة بالمستهلك.

فرض تشريعات تتماشى مع المستجدات القانونية لمواجهة أخطار البيئة الإلكترونية قصد مواجهتها فنيا وتقنيا حتى نتمكن من الوصول إلى تخصيص تشريعات مهمة تتعلق بتنظيم وسائل المعاملات الإلكترونية وكذا الأعمال المرتبطة بها.

العمل على توفير الحماية التقنية التي تتلاءم مع الأمن القانوني في هذا الجانب مما يتطلب حماية كافية للتجارة الإلكترونية، وتكوين فرق بحث تتكون من خبراء قانون وخبراء تقنيين يعملون على فحص الجزئيات من أجل الوصول إلى فرض تشريعات قانونية مرتبطة بالتجارة الإلكترونية إلى جانب تفعيل فنيات الاتصال للمعلومة.

قائمة المصادر والمراجع

أولاً: باللغة العربية

- الكتب:

- 1- إبراهيم بخي، التجارة الإلكترونية، مفاهيم واستراتيجيات التطبيق في المؤسسة، ديوان المطبوعات الجامعية، الجزائر، 2005.
- 2- دانون سمير، العقود الإلكترونية في إطار تنظيم التجارة الإلكترونية، المؤسسة الحديثة للكتاب، لبنان، 2012.
- 3- سليمان ضيف الله الزبن، التحويل الإلكتروني للأموال ومسؤولية البنوك القانونية، دار الثقافة للنشر والتوزيع، الأردن، 2012.

- 4- عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، دار الفكر الجامعي، مصر، 2004.
- 5- علي أحمد نعمان، الحماية التقنية للتجارة الإلكترونية، مجلة القانون، عدد 1، مطبعة وراقة وطنية، المغرب، 2011.
- 6- عمر خالد زريقات، عقد التجارة الإلكترونية (عقد البيع عبر الأنترنت- دراسة تحليلية)، دار حامد للنشر والتوزيع، عمان، الأردن، 2007.
- 7- محمود محمد أبو فروة، الخدمات البنكية الإلكترونية عبر الإنترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2009.
- 8- فاروق محمد الأباصيري، عقد الاشتراك في قواعد المعلومات عبر شبكة الانترنت، دار الجامعة الجديدة القانونية، الإسكندرية، مصر، 2002.
- 9- هدى حامد قشقوق، الحماية الجنائية للتجارة الإلكترونية عبر الأنترنت، دار النهضة العربية، مصر، 2000.
- 10- يمينه حوحو، عقد البيع الإلكتروني في القانون الجزائري، دار بلقيس، الجزائر، 2016.

ثانياً:- الرسائل والمذكرات الجامعية:

أ- رسائل الدكتوراه:

- 1- بهلولي فاتح، النظام القانوني للتجارة الإلكترونية في ظل التشريع الجزائري أطروحة لنيل درجة الدكتوراه في العلوم، تخصص قانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 2017.

ب- مذكرات الماجستير:

- 1- لزعر وسيلة، تنفيذ العقد الإلكتروني، مذكرة لنيل شهادة الماجستير في القانون، فرع العقود والمسؤولية، كلية الحقوق، جامعة الجزائر (1)، بن عكنون، 2010.
- 2- بلقاسم عبد الله، المحررات الالكترونية وسيلة لإثبات العقد الإلكتروني (دراسة مقارنة)، مذكرة لنيل شهادة الماجستير في القانون، فرع القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة تيزي وزو، 2013.

ثالثاً:- المقالات والملتقيات:

- 1- أحمد محمد عصام الدين، "ماذا تعرف عن عملة البيتكوين Bitcoin"، مجلة المصري،

- إدارة البحوث والتنمية، عدد 73، سبتمبر 2014، ص ص 50-53.
- 2- حمد زيدان، أسباب تدفعك لشراء بتكوين وأخرى تحذرك من الاتجار بها، 4 جانفي 2008، تم الاطلاع عليه يوم 03 سبتمبر 2024 الساعة 23:15 متوفر على الرابط: <http://bit.ly/38+lbQo>
- 3- حسن محمد مصطفى، دور عملة البيتكوين في تمويل وتنظيم الجماعات الإرهابية، صحيفة حفريات، مركز دال للإنتاج والأبحاث والإنتاج الإعلامي، مصر، 2017، تم الاطلاع عليه يوم 05 سبتمبر 2024، الساعة 00:28 ص 13 متوفر على الرابط: <http://bit.ly/38ttduD>
- 4- نور الدين صويلحي، أثر البيتكوين والعملات الافتراضية على استقرار النظام النقدي العالمي، مجلة آفاق علمية، المركز الجامعي بتمنراست، الجزائر، المجلد 10، عدد 2، سنة 2018، ص ص 219-239، ص 227

الملتقيات:

- 1- حليتييم سراح، حماية المعاملات القانونية على تقنية التشفير الإلكتروني، ضمن فعاليات الملتقى الوطني حول الإطار القانوني للتوقيع والتصديق الإلكترونيين في الجزائر، يومي 12 و13 جانفي 2016، بجامعة محمد الشريف مساعديه، سوق أهراس.

4- النصوص القانونية

- قانون رقم 04-09 مؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ج ر ع 47، صادر بتاريخ 16 غشت 2009.
- 17- قانون رقم 15 - 04 مؤرخ في 11 ربيع الثاني 1436هـ/الموافق ل 1 فبراير 2015 يحدد القوانين العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج ر، عدد رقم 6 صادر في 10 فبراير 2015