التّشفير وسيلة لتأمين التجارة الإلكترونية من المخاطر التقنية

Encryption, a means to secure electronic commerce from technical risks

عرعار الياقوت

مخبر الدولة والإجرام المنظم: مقاربة قانونية وحقوقية بأبعاد اقتصادية واجتماعية، كلية الحقوق والعلوم السياسية، جامعة البويرة، الجزائر.

l.arar@univ-bouira.dz

تاريخ الاستلام: 2021/07/07 تاريخ القبول للنشر: 2021/12/21

****

ملخص:

ممّا لا شك فيه أنّ التجارة الإلكترونية حقّقت الكثير من الفوائد بالنسبة للشّركات والزبائن على حدّ السّواء، وأصبح العالم اليوم أمام ثورة معلوماتية هائلة، مسيطّرة على عناصر الإنتاج في مختّلف أوجه النشاطات الاقتصادية، تمكّن الشّخص من عقد الصّفقات التّجارية أو الحصول على المعلومة في أيّ موضوع ومن أي مكان، بسرعة فائقة وتكلفة منخفضة. ومع هذا التّطور المذهل والسّريع، دقّ ناقوس الخطر في كيفية حماية تلك المعلومات المرسّلة بين الجهات المختّلفة.

ومن أجل حماية أمن المعلومات عامة وأمن التجارة الإلكترونية خاصة، سعت الكثير من الدول لإيجاد تقنيات لضمان خصوصية تعاملات الأطراف ومنع أية تعدّيات عليها؛ ويعدّ التّشفير من أكثر الحلول قدرة على النجاح لحلّ مشكلة تأمين المعاملات الإلكترونية.

الكلمات المفتاحية: التجارة الإلكترونية؛ المفتاح العام؛ المفتاح الخاص؛ خوارزميات رياضية؛ فك الشّفرة.

Abstract:

In light of the massive information revolution that the world is witnessing today, electronic commerce has, without any doubt, achieved a lot of benefits for both businesses and customers by dominating the factors of production in various aspects of economic activities, it enables a person to conclude business deals or get information anywhere and about any topic, at high speed and low cost.

Despite this huge and rapid development, the danger remains on how to protect this information transmitted between different parties.

In order to protect data in general and electronic commerce in particular, many countries have sought to develop techniques to ensure

the privacy of the parties' transactions and prevent its invasion; Encryption is one of the most successful solutions aimed at securing electronic transactions.
key words: Electronic commerce; Public key; Private Key; Mathematical algorithms; Decryption.

مقدمة:

تعدّ المعلومات وتقنياتها أهم عناصر البنية الأساسية للتّنمية الاقتصادية والاجتماعية في العصر الذي نعيش فيه، إذ أصبحت المعلوماتية القوة المسيطّرة على عناصر الانتاج في مختّلف أوجه النّشاطات الاقتصادية والمتمثّلة في التّجارة الإلكترونية.

فانتشر التّسوق الإلكتروني والشّراء عبر شبكة الأنترنت في كل بلدان العالم المتقدّم، بحيث بلغت مبيعات بعض المواقع الأمريكية واليابانية أرقام فلكية؛ أدّت إلى تغيير جذري في هيكل التّجارة وسوق الوظائف في تلك البلدان، وكانت هذه المبيعات نتيجة مباشرة لقوة الإعلانات ورخص الأسعار وخلوّها من الضّرائب، ولكن السّبب الأقوى والخفي وراء هذه الظّاهرة هو اعتماد تلك المواقع على تكنولوجيا متطوّرة، لتأمين سلامة وسرّية المعلومات المطلوبة لإتمام عملية الشّراء؛ مما زاد من الثّقة بأمن وسرّية التّعاملات الخاصّة بالشّراء من على الشّبكة.

من أجل مواجهة المخاطر التّي تقابل الأشخاص المتعاملين في مجال التجارة الإلكترونية، وُجدت بعض الحلول التّقنية التّي توفّر الأمان واليقين القانونيين لهؤلاء الأشخاص؛ وتتمثّل هذه الحلول في تشفير البيانات المتبادلة إلكترونيًا، من هنا نجد أنّ كل فرد أو شركة أو هيئة تجارية بحاجة للتّشفير، للحفاظ على خصوصياتها وأسرارها ومعلوماتها الهامة جدًّا من أن يطّلع عليها أحد، ولمنع مرتكبي جرائم الاختراق والاحتيال الإلكتروني من ارتكاب جرائمهم في هذه التّعاملات الإلكترونية. كما أنّ وسيلة حماية سلامة المحتوى تقوم على تشفير البيانات المتبادلة، والتّثبت لدى فك التّشفير أنّ الرسالة الإلكترونية لم تتعرّض لأي نوع من التّعديل أو التّغيير، وبذلك فإنّ التّشفير يمثّل الاستراتيجية الشّمولية لتحقيق أهداف الأمن من جهة، و من جهة أخرى هو مكوّن رئيس لتقنيات ووسائل الأمن الأخرى؛ خاصّة في بيئة الأعمال الإلكترونية والتجارة الإلكترونية والرسائل الإلكترونية، وعموما البيانات المتبادلة بالوسائط الإلكترونية. ومن هذا المنطلق يمكن طرح الإشكالية التّالية: **كيف يساهم التّشفير في ضمان الثّقة وتأمين معاملات التجارة الإلكترونية؟**

وعليه فقد تمّ تقسيم الدراسة إلى مبحثين: بيّنا في **المبحث الأول** الإطار المفاهيمي للتّشفير الإلكتروني من خلال دراسة التعريف بالتّشفير الإلكتروني في مطلب أول وأساليب التّشفير الإلكتروني في مطلب ثاني، أما **المبحث الثاني** فقد كان مخصّصا لدراسة أحكام نظام التّشفير الإلكتروني، ولأجل بيان ذلك قسّمنا هذا المبحث إلى مطلبين، لنعرض في الأول خصوصيّة البيانات المشّفرة، وفي المطلب الثاني سنبحث فيه النظام الفنّي للتّشفير الإلكتروني.

المبحث الأول: الإطار المفاهيمي للتّشفير الإلكتروني

أشارت العديد من الدراسات على مدى السّنوات الماضية إلى أنّ غالبية المتعاملين عبر شبكة الأنترنت قلقون في تحديد شخصية الطّرف الثّاني، وصّحة المعلومات التّي ترد عن طريق شّبكة الأنترنت، ومدى صّحة العروض التّي تطرحها الشّركات، ومدى حجية وكيفية السّيطرة على خصوصياتهم في التّعاقد عبر الأنترنت، لذلك ظهرت التّقنية الشّائعة المستّعملة في التّوقيع الرّقمي وهي تقنيّة التّشفير. وعليه سنقصّر نطاق بحثنا في هذا المبحث على التّعريف بالتّشفير الإلكتروني (**المطلب الأول**)، ثم التّطرّق إلى أساليب التّشفير الإلكتروني (**المطلب الثاني**).

المطلب الأول: التّعريف بالتّشفير الإلكتروني

يعتّبر التّشفير من وسائل حفظ سرّية المعلومات- لاسيما في التجارة الإلكترونية- التّي تتطلّب الحفاظ على البيانات ومعاملات الأطراف، وحجم الصّفقات ونوعها وكذلك حماية النقود المُتداولة داخل هذه التّجارة. فالتّشفير يهدف إلى منع الغير من الدّخول والتقاط رسائل البيانات؛ التّي يتّم تبادلها من خلال شبكة الأنترنت. وعليه لبيان ذلك نرى تقسيم هذا المطلب إلى فرعين؛ نتحدّث في **الأول** عن تطور علم التّشفير وأهميّته، و**الثّاني** نُورد فيه المقصود بالتّشفير الإلكتروني.

الفرع الأول: تطور علم التّشفير وأهميّته

التّشفير كوسيلة هامة من وسائل حماية الرسائل الإلكترونية هي عملية تمويه الرسالة؛ بطريقة تخفي حقيقة محتواها وتجعلها رموزًا غير مقروءة، و تسمّى كذلك عملية التّرميز ،وهي تتضمّن تطبيقات لمعاملات ودوال رياضية على نص إلكتروني ينتّج عنه مفتاح تشفير؛ يجعل المعلومات غير قابلة لفك تشفيرها من قِبل أي شخص لا يملك مفتاح فكّ التّشفير المناسب (**علي، 2019، صفحة 76**). وفي نفس الصّدد يُعرّف علم التّشفير بأنّه: "علم الكتابة السرّية وعدم فتح شفرة هذه الكتابة السرّية من قِبل غير المخولين" (**عوض ، 2005، صفحة 34**). لذا سنقوم بالتطرّق لتطوّر علم التّشفير(**أولا**)، ثم نبرز أهميّته (**ثانيا**).

أولا- تطور علم التّشفير: يعتّبر نظام تشفير البيانات من أول الأنظمة الدّفاعية التّي يمكن استخدامها لتجنّب حدوث الأزمة، ويستّهدف هذا النظام تحقيق قدر معقول من الأمان والحماية لتأمين التّعاملات التّجارية داخل الشّبكة. وقد انتّشر استخدام نظام الشّفرة قديمًا وخاصّة في المجالات الحربية والعسكرية **(السبكي ، 2000، الصفحات 393-394)**، ويرجع علم التّشفير إلى عام 1466حيث كتب العالم Leon Alberti مقال عن نظرية فن الأبعاد الثّلاثي في الرّسم، ولقد قام ألبرت بعمل جدول للشّفرة، ثمّ حاول أن يطوّر نفسه وأن يجمع بين نظام التّشفير والكود؛ بمعنى أن يتّم إعداد كتاب توضع فيه عبارات وجمل طويلة، ويضع أمامها كود سرّي مكوّن من عبارة ليس لها معنى، ليقوم بعد ذلك الشّخص بتشفير الكود باستخدام الجدول الذي أعدّه ألبرت. ومثال ذلك أن يُوضع أمام عبارة "يجب التّخلص من المخدرات وعدم الاتصال بي" كود؛ وليكن مثلا كلمة " الإعدام"، ثم يقوم المشفِّر بعمل شفرة لكلمة الإعدام، واستبدال الأحرف المكوّنة لها بأحرف أخرى أو اختزال بعضها، بحيث تصبح كلمة الإعدام "عد" مثلا، وهكذا في كل العبارات والجمل التّي تستّخدّم بكثرة **(الرومي، 2008، صفحة 34)**.

وتجدر الإشارة أنّ التّشفير تمّ استخدامه الآن في مجال التجارة الإلكترونية؛ وكانت بداية التّفكير في عمليات التّشفير على يد شركة IBM في أواخر السّتينيات؛ عندما نجحت في تطوير نظام تشفير حقّق انتشارًا واسعًا في الأسواق، ثمّ بدأت الشّركات بعدها بتطوير أنظمة تشفير جديدة، ممّا أبرز الحاجة إلى وجود معيار لعمليات التّشفير ،إلى أن طُوّر برنامج التّشفير عام 1986 إلى برنامج يعتّمد نظام RSA، وهو من أكثر برامج التّشفير انتشارًا **(المزيني، 2018، صفحة 275)**.

ثانيا- أهمية التّشفير الإلكتروني: تبرز أهمية التّشفير بعد زيادة معدّل التّبادل التّجاري عبر شبكة الأنترنت ووجود التجارة الإلكترونية، حيث أصبح هناك ما يُعرف بالقراصنة الذين يقومون بالاعتداء على الرسائل، لذلك برزت أهمية التّشفير من خلال حماية البيانات والأعمال والمراسلات والتّحويلات المالية، التّي يتّم تداولها من خلال شبكة الأنترنت، كذلك يعتّبر التّشفير من الدّعائم الأساسية التّي تقوم عليها التجارة الإلكترونية؛ لاكتساب ثقة المستّهلك وإدخال الطّمأنينة عليه، وحتّى لا تكون بياناته عرضة للاختراق **(البياتي، 2014، صفحة 250)**. ولابدّ من الإشارة أنّ فكرة أي نظام تشفير تتمثّل في إخفاء المعلومات السّرية، بطريقة يصبح من خلالها معناها غير مفهوم بالنسبة إلى أيّ شخص غير مصرّح له بالاطلاع

عليها. وفي هذا المقام يتمثّل الاستخدامان الأكثر شيوعًا للتّشفير في تخزين البيانات بأمان في ملف كمبيوتر، أو نقلها عبر قناة غير آمنة مثل الأنترنت، وبناء على ذلك في كلتا الحالتين حقيقة كون المستّند مُشفّرًا؛ لا تمنع الأشخاص غير المصرّح لهم بالوصول إليه، ولكنّها تضمن عدم تمكّنهم من فهم ما يرونه. في مقام موالي غالبًا ما يطلّق على المعلومات المُراد إخفاؤها اسم النّص الأصلي، فيما يطلّق على عملية إخفائها اسم التّشفير، ويُطلق على النص الأصلي المشفّر اسم " النّص المشفّر" أو "بيان التّشفير"، كما يطلّق على مجموعة القواعد المستّخدّمة في تشفير معلومات النّص الأصلي "خوارزمية التّشفير"، ولكن لا يفوتنا أن ننوّه أنّ هذه الخوارزمية عادة تعتّمد على مفتاح التّشفير؛ وهو يمثّل مدخلاً لها بالإضافة إلى الرسالة، وحتى يتمكّن المتلقي من استرجاع الرسالة من خلال النّص المشفّر، يجب أن تتوافر خوارزمية فك التّشفير؛ التّي عند استخدامها مع مفتاح فكّ التّشفير المناسب تستّرجع النّص الأصلي من النّص المُشفّر (**بايبر و ميرفي، 2016، صفحة 15**).

الفرع الثاني: تحديد المقصود بالتّشفير الإلكتروني

بادئ ذي بدء يُقصد بوسائل أمن المعلومات هي مجموعة من الآليات و الإجراءات والأدوات والمنتجات؛ التّي تستّخدم للوقاية من أو تقليل المخاطر والتّهديدات التّي تتعرّض لها الكمبيوترات والشّبكات، وبالعموم نظم المعلومات وقواعدها (**الشّحات، 2010، صفحة 166**). فالتّشفير ما هو إلاّ منظومة تقنية حسابية، تستّخدّم مفاتيح خاصة لمعالجة وتحويل البيانات والمعلومات المقروءة إلكترونيًا، بحيث لا يستّطيع أي شخص الوصول إلى تلك البيانات إلاّ عن طريق استخدام مفتاح أو مفاتيح تلك الشّفرة (**يوسف، 2008، صفحة 52**). لذا سنقوم بإيراد بعض الاتجاهات الفقهية التّي اهتّمت بتحديد المقصود منه(**أولا**)، ثمّ التّطرق لمعناه من النّاحية الفنيّة(**ثانيا**)، لنصل إلى الإشارة لأهم التّشريعات التّي تطرقت بالدراسة له سواءً العربية المُقارِنة منها أو الدّولية(**ثالثا**).

أولا- المقصود بالتّشفير من النّاحية الفقهية: أما الفقه فقد عرّف البعض منه التّشفير بأنّه: "تغيير في شكل البيانات عن طريق تحويلها إلى رموز أو إشارات، لحماية هذه البيانات من إطلاع الغير عليها أو من تعديلها أو تغييرها." (**العبيدي ، 2012، صفحة 157**). وفضلاً عن ذلك عرّف جانب من الفقه التّشفير بأنّه: "هو عملية الحفاظ على سرّية المعلومات، باستخدام برامج لها القدرة على تحويل وترجمة تلك المعلومات إلى رموز، بحيث إذا ما تمّ الوصول إليها من أشخاص غير مخوّل لهم بذلك، لا يستّطيعون فهم أي شيء لأنّ ما يظهر لهم هو خليط من

الرموز والأرقام والحروف غير المفهومة، وهي طريقة عملية لحماية المعلومات التّي تنقّل من خلال شبكات الاتصال، ويمكن استخدامها لغرض صلاحية وسلامة الرسائل، والحماية من مرسّل الرّسالة الذي ينكّر الإرسال لاحقًا." **(جراح، 2009، الصفحات 194-195)**.

أو أنّ التّشفير "Encryption" هو: ((عملية تحويل المعلومات إلى رموز، بحيث تصبح محمية من عمليات الوصول غير المُرخّص بها؛ باستخدام برنامج مفتاح تشفير قبل إرسال الرسالة، وتكون لدى المستّقبِل قدرة استعادة الرسالة الأصلية بعملية عكسّية لفك التّشفير "Decryption"، والهدف هو جعل المعطيات المخزّنة والمعطيات التّي يجري نقلها على الأنترنت آمنة، ثمّ إنّ عملية التّشفير تحقّق تكاملية الرّسالة وتحقّق عدم النكران والتّوثّق والسّرية)) **(أمحمد بن الدين، محمد و حليمي، 2007، صفحة 10)**. علاوة على ذلك عرّف البعض التّشفير بأنّه: "تغيير في شكل البيانات عن طريق تحويلها إلى رموز أو إشارات، لحماية هذه البيانات من إطلاع الغير عليها؛ من تعديلها أو تغييرها." **(الرومي، 2008، صفحة 32)**.

كما عُرّف: "تشفير المعلومات هو تغيير مظاهرها بحيث يختّفي معناها الحقيقي." **(Bowers, 1988, p. 51)**.

ثانيا- المقصود بالتّشفير من النّاحية الفنيّة: ذهب البعض إلى اعتماد تعريف للتّشفير من النّاحية التّقنية أو الفنيّة بأنّه: " التّشفير أو التّرميز أو الكتابة المُشفّرة هو تقنية قوامها خوارزمية رياضية ذكية، وبالعكس تسمح لمن يمتّلك مفتاحًا سرّيًا بأن يحول رسالة مقروءة إلى رسالة غير مقروءة، أي أن يستّخدم المفتاح السّري بفك الشّفرة وإعادة الرّسالة المشفّرة إلى وضعيّتها الأصلية." **(الجواري، 2010، صفحة 202)**.

هكذا يتبيّن أنّ التّشفير من النّاحية الفنيّة يعني إعادة كتابة رسالة البيانات قبل إرسالها؛ باستخدام مفتاح معيّن يفتّرض الرّبط بين البيانات والأرقام، على أن تتوافر لدى المُرسَّل إليه القدرة على استعادة الرّسالة في صورتها الأصلية قبل تشفيرها، وذلك إمّا باستعمال المفتاح ذاته الذي استّعمله المُرسّل، أو باستعمال مفتاح آخر على حسب نوع التّشفير المستّعمل **(بومحراث، 2019، الصفحات 289-290)**.

لابدّ من الإشارة أنّ الفكرة الأساسية لتكنولوجيا التّشفير هي تحويل رسالة البيانات المكتوبة على جهاز الكمبيوتر، باستخدام برنامج تشفيري معيّن إلى معلومات أو إشارات غير مفهومة بالنسبة للغير، ثمّ بعد ذلك تنتّقل هذه الرّسالة إلى حاسوب الشّخص المستّقبِل؛ الذي يستّخدّم تكنولوجيا معيّنة أيضًا - تسمى تكنولوجيا فك التّشفير- لتحويل الرّسالة غير

المفهومة إلى وضعها الأصلي كرسالة مقروءة ومفهومة (**عبيدات و درادكة ، 2009، صفحة 47**). استنادا إلى ما سبق فإنّ التشفير الإلكتروني يحتاج إلى نظام ترميز مصمّم من قِبل التّقنين بواسطة أجهزة الحاسوب، مستّخدما فيها برامج كمبيوترية معقّدة بواسطة مفاتيح؛ مختارة ضمن بروتوكولات مرخّصة أو معتّمدة (**زريقات، 2007، صفحة 271**).

ثالثا- المقصود بالتّشفير من النّاحية القانونية: في هذا الصّدد تباينت تعريفات التّشريعات للتّشفير؛ فمنهم من عرّف هذه العملية في نصوص التّشريعات، ومنهم من أشار إليها بطريقة غير مباشرة مثل قانون الأونسيترال بشأن التّوقيعات الإلكترونية الذي لم يشر إلى تعريف مباشر للتّشفير ؛إنّما ذكره كجزء من التّوقيع الرّقمي الذي يرتّكز بالأساس على عملية التّشفير. كما قام البرلمان الأوربي بتاريخ 1999/04/13 بالموافقة على تقرير المفوضية حول تطبيق التّنظيم رقم 3381/1994 بتاريخ1994/12/19؛ والمعدّل بالتّنظيم رقم 837/95 بتاريخ 1995/04/10 المقترّح من الدول الأعضاء؛ والمتعلّق بإحداث نظام مراقبة لتصدير المواد ذات الاستعمال المزدّوج، ويرمي هذا التّقرير إلى إلغاء القيود القائمة على تداول تقنيات ومنتجات التّشفير فيما بين الدول الأوربية والأعضاء (**الجنابي، 2009، صفحة 33**).

في مصر لم يتعرّض قانون التّوقيع الإلكتروني المصري إلى تعريف التّشفير، لكن مشروع قانون التجارة الإلكترونية المصري رقم2001 وضع تعريفا للتّشفير في الفصل الأول منه "التعريفات"؛ حيث عرّفه على أنّه: " تغيير في شكل البيانات عن طريق تحويلها إلى رموز أو إشارات، لحماية هذه البيانات من إطلاع الغير عليها أو من تعديلها أو تغيرها." (**المطالقة، 2006، صفحة 159**). في حين أورد المشرّع المغربي من خلال الكتاب الثالث تعريفا للتّشفير في المادة 12 من قانون 53/05(**قانون 53/05 ، 2007، صفحة 3879**) بأنّه: " وهو كل جهاز أو برنامج معلوماتي مستوحى أو معدّل بغرض تحويل معطيات سواء كانت معلومات أو إشارات، ومن خلال اتفاقات سرّية أو بغرض إنجاز عكس تلك العملية باتفاق سرّي أو بدونه ". ويُلاحظ أنّ هذا التّعريف الذي أورده المشرّع المغربي قريب من التّعريف الذي أورده المشرّع الفرنسي (**أنجوم و الحياني، 2007، صفحة 101**).

في مقام موالي عرّفه المشرّع التونسي في المادة05/02 من قانون المبادلات والتجارة الإلكترونية التّونسي (**قانون المبادلات والتجارة الإلكترونية التونسي رقم 83، 2000**) بأنّه: "استعمال رموز أو إشارات غير متداولة تصبح بمقتضاها المعلومات المرغوب تحريرها أو إرسالها غير قابلة للفهم من قِبل الغير، أو استعمال رموز أو إشارات لا يمكن وصول المعلومة

بدونها". ويُلاحظ في هذا التعريف أنّ المشرع التونسي بيّن أنّ الغرض من التّشفير هو منع الغير من الاطلاع على معلومات معيّنة؛ تتعلّق بالمعاملات التّي تتّم عبر الأنترنت، وأيضا عدم إمكانية الاطلاع حتى من قِبل المُرسَّل إليه (المُستّقبِل) إلاّ عن طريق فك رموز الشّفرة، وناهيك عن ذلك هذا التّعريف يشابه إلى حدّ كبير تعريف المشرّع المصري للتّشفير في مشروع التجارة الإلكترونية **(الجنابي، 2009، الصفحات 34-35)**.

على خلاف ذلك لم يتطرّق المشرّع السّعودي للمقصود بالتّشفير في نظام التّعاملات الإلكترونية السّعودي. وتجدر الإشارة أنّ باقي التّشريعات العربية التّي تعاملت مع التجارة الإلكترونية، تطرّقت إلى تقنية التّشفير بشكل غير مباشر؛ وذلك من خلال تطرقها للتّوقيع الإلكتروني الذي يعتّمد بشكل أساسي على عملية التّشفير **(العبيدي ، 2012، صفحة 157)**، فالمشرّع الأردني لم يتعرّض للتّشفير بطريقة مباشرة؛ ولذلك لم يرد تعريف له في قانون المعاملات الإلكترونية **(الصباحين، 2005، صفحة 65)**.

في مقام موالي وبالرجوع إلى التّشريع الجزائري نجد أنّ القانون رقم15/04 **(قانون** 04/15، 2015)لم يعرّف التّشفير، وإنّما تطرّق إلى المقصود بمفتاحي التّشفير العام والخاص، فعرّف مفتاح التّشفير الخاص في المادة 02 فـ08 على أنّه: "عبارة عن سلسلة من الأعداد يحوزها حصريًا المُوقّع فقط، وتُستّخدم لإنشاء التّوقيع الإلكتروني، ويرتّبط هذا المفتاح بمفتاح تشفير عمومي" . ومن زاوية أخرى، يقصد بمفتاح التّشفير العمومي حسب ما ورد في المادة 02 فـ09 بأنّه: "عبارة عن سلسلة من الأعداد تكون موضوعة في متناول الجمهور بهدف تمكينهم من التّحقق من الإمضاء الإلكتروني وتدرج في شهادة التّصديق الإلكتروني".

المطلب الثاني: أساليب التّشفير الإلكتروني

تجدر الإشارة أنّ تقنية التّشفير تعتّمد ببساطة على تشفير الرسالة عند قيام المُرسّل بإرسال الرسالة للمرسَّل إليه، كما يستّخدم برنامج محدّد يسمى بمفتاح التّشفير لاختيار شفرة معيّنة؛ يتّم وضعه قبل إرسال الرّسالة، على أن تكون لدى المُرسَّل إليه وهو مستّقبِل الرّسالة القدرة على استقبال الرسالة في صورتها الأولى قبل التّشفير ؛باستخدام العملية العكسية للتّشفير **(السبكي ، 2000، الصفحات 393-394)**.

تأسيسًا على ذلك نجد أنّ معظم عمليات التّشفير المعروفة حتّى هذا الوقت، تعتّمد أنواع من أساليب أو تقنيات التّشفير يتّم استخدامها في التجارة الإلكترونية، وهذا ما سوف

نناقشه من خلال الفرعين التّاليين: فيتناول **الفرع الأول** تقنية التّشفير المتماثل، أمّا **الفرع الثاني** فيتحدث عن التّشفير غير المتماثل.

الفرع الأول: تقنية التّشفير المتماثل

هذه الطريقة للتّشفير تسمى "التّشفير السيمتري"، وقد استّخدم في البداية التّشفير المتماثل لتشفير التّوقيع الإلكتروني الرّقمي، و بمقتضاه يكون لكل من مصدّر الرسالة والمُرسَّل إليه نفس مفتاح التّشفير لفكّ رموزها، وقبل إرسال الرسائل المشفّرة يتّم إرسال مفتاح التّشفير إلى المُرسَّل إليه بطريقة آمنة ليستّطيع فكّ الشّفرة (**هالة ، 2013، صفحة 345**)، فمُصدّر الرسالة وهو هنا المستهلك والمُرسَّل إليه الذي هو التاجر أو مورّد الخدمة يستّخدمان نفس مفتاح التّشفير لفكّ رموزها، وقبل إرسال الرسائل المشفّرة يتّم إرسال مفتاح التّشفير إلى المُرسَّل إليه بطريقة آمنة ليستّطيع فكّ الشّفرة (**نعمان، 2015، صفحة 66**). ومثال ذلك: إذا أراد شخص أن يرسل نصًا إلى شخص آخر فعليه إرفاق الرّسالة بمفتاح وجدول للرموز، إضافة إلى تحديد العدد الأقصى للرموز المستّعملة "MODULE"، فاذا استّعمل أحرف اللّغة العربية فتكون القيمة هي 28، إذن نستّعمل28 "MODULE"، وهذا لكي لا نتحصل حين تشفير الرسالة أو فكّها على قيمة تجاوز عدد الأحرف المستّعملة، و التّي لا يكون لها حرف يقابلها (**حليتيم، 2018، صفحة 740**).

يحقّق نظام التّشفير المتماثل عدة مزايا لكونه لا يحتاج إلى حواسب آلية ذات قيمة عالية، كما أنّه يتّسم بالسّرعة والسّهولة في إجراء عملية الإغلاق وفتح بيانات المحرّر الإلكتروني (**ربضي، 2009، صفحة 68**).

ما يؤخذ على هذا النظام بأنّ على مُتلقي الرسائل المُشفّرة من مصادر مختلفة؛ اقتناء عددا من المفاتيح الخصوصية يوازي عدد مرسليها، كما أنّه لا يحتّوي على حيطة من حيث أسلوب تبادل رموز هذه المفاتيح بين المتعاملين، إضافة إلى أنّ استخدام ذات المفتاح من قِبل المُرسّل والمُرسَّل إليه يُضعف من حجية المحررات المستّخرجة ويُضعف قوتّها الثّبوتية، وذلك بالنّظر إلى مستوى المخاطر في تسريب أو انتقال شفرة المفتاح الخصوصي إلى الغير (**زريقات، 2007، الصفحات 271-272**).

الفرع الثاني: تقنية التّشفير غير المتماثل

يسمى نظام المفتاح المُتباين وهو عبارة عن سلسلة من الهندسة العكسية (Algarithm)، ويستّخدم فيها مفتاحين مختّلفين أحدهما للتّشفير والآخر لفك الشّفرة،

ويتمتّع المفتاحين بخاصية هامة هي أنّه لو عُرف إحدى هذين المفتاحين لا يمكن معرفة المفتاح الآخر حسابيًا، وكل مفتاح سواء المفتاح العام أو الخاص يحمل علامة رياضية معقّدة لا يمكن معرفتها إلاّ من جانب صاحبها، والمفتاح الخاص لا يتصور معرفة شخص آخر به غير صاحبه؛ فهو يظل سرّا على الآخرين، أما المفتاح العام فيمكن معرفته لبعض الجهات المختّصة **(محمد أمين، 2004، صفحة 31)**.

تعتّمد هذه التّقنية على تقنيات تشفير البيانات وبعثرتها Scrabling، استنادًا إلى علاقات رياضية خاصة، تجمع ما بين مفتاحين- أو بالأحرى كلمتين سرّيتين -أحدهما عام والآخر خاص. فمثلاً عند إرسال رسالة يقوم التّطبيق الموجود على جهاز ي بتشفيرها، أو بعثرة بياناتها باستخدام كلمة سر غير معروفة لأحد سواي، ثم تشفيرها ثانية بالمفتاح العام للمستّقبل، والسّبيل الوحيد الذي يمكن به المستّقبل أن يتعامل مع هذه الرسالة يتمثّل في فكّ تشفيرها، أو إعادة ترتيب بياناتها باستخدام مفتاحه الخاص أو كلمته السّرية أولاً، ومن ثمّ استخدام مفتاحي العام لفكّ شيفرتي الخاصّة. وتقوم هيئات عالمية وشركات خاصّة بإصدار شهادات رقمية للمصادقة على صّحة هذه المفاتيح؛ ومنها شركات مثل RSA أو Veri Sign **(الألفي، 2010، صفحة 193)**.

إنّ استعمال المفتاح العام للمُرسّل من قِبل المُستّقبل لفكّ شيفرة التّوقيع الرّقمي، وملخص الرّسالة وإخراج قيمة التّمويه؛ يضمن أنّ هذه الرّسالة قد أُنشئت من قِبل حامل المفتاح السرّي المحاكي للمفتاح العام للمُرسّل، وبالتّالي يضمن شخصية المُرسّل. كما أنّ أي تغيير في محتوى الرّسالة سوف ينتّج عنه اختلاق في قيمة التّمويه، ممّا سوف يؤدي إلى عدم فكّ شيفرة الرّسالة؛ الأمر الذي يضمن سلامة الرّسالة **(المومني، 2003، صفحة 58)**. وجدير بالذّكر مع ذلك أنّ مفهوم التّرميز بالمفتاح العمومي لا ينطوي بالضّرورة على استخدام الخوارزميات السّابقة الذكر المبنيّة على الأعداد الأولية، ذلك أنّه توجد في الوقت الراهن تقنيات رياضية أخرى تستّخدم أو قيد التّطوير، يذكر منها نظم التّرميز التّي تعتّمد على المنحنيات الأهلية، والتّي كثيرا ما يقال أنّها تتيح درجة عالية من الأمان من خلال استخدام مفاتيح مخفّضة الطول تخفيضًا كبيرًا **(يوسف، 2008، صفحة 55)**.

حسب هذا النظام غير المتماثل يتّم تبادل الرّسائل المشفّرة عبر شبكة الأنترنت من خلال برامج مثل Netscape وDigicash، إضافة لنظام PGP الذي كان له الفضل في الكشف عن نظام أحدث يسمى "clipper ship" التّشفير الائتماني النّموذجي؛ الذي جرى وضعه من

قبل وكالة الأمن القومية الأمريكية لاستخدامه في مجال المعدّات الإلكترونية (زريقات، 2007، الصفحات 272-273).

هكذا يتبيّن أنّ التّشفير غير المتماثل يحافظ على سرّية رسالة البيانات، ولكنّه وحده لا يساعد على التّعرف على مُصدّر الرّسالة الذي يستّطيع أن يجحدها، كما لا يحول دون التّلاعب في فحواها، فقد يلتّقط الغير الرّسالة ليعدّل في مضمونها ثمّ يطلقها من جديد، دون أن يترك شاهدًا على التّحريف.

وبناء على ذلك يحتاج نظام التّشفير غير المتماثل إلى قنوات اتصال إلكترونية خاصّة، ويتوقّف نجاحه على مدى تعقيد النّمطية الرياضية" Algorithme mathématique" المستّخدمة في اشتقاق مفاتيح التّشفير **(Bensoussan & Le Roux, 1999, p. 18)**.

يجب عدم الخلط بين التّوقيع الإلكتروني وتشفير الرّسالة الإلكترونية؛ فإذا كان كلاهما يقوم على عملية حسابية يتّم من خلالها تشفير مضمون التّوقيع والرّسالة، لكنّهما يختّلفان في أنّ تشفير الرسالة يشملها بأكملها، في حين أنّ التّشفير في التّوقيع الإلكتروني يقتّصر على التّوقيع دون بقية الرّسالة؛ بحيث يمكن أن يرتّبط التّوقيع برسالة غير مشفّرة (هالة ، 2013، صفحة 346).

في واقع الأمر هناك من يستّعمل تقنية التّشفير المُزدّوج - المزج بين نظامي المفتاح المتماثل والمفتاح العام -؛ إذ بمقتّضى هذا النظام سنتجاوز سلبيات كل من الأنظمة السّابقة، حيث سنتغلب على مشكلة إرسال المفتاح المتماثل عبر قنوات آمنة لحلّ شفرة الرّسالة من ناحية، واقتصار الوقت في تشفير رسالة البيانات باستخدام المفتاح العام وحلّها من ناحية ثانية. ويُلاحظ أنّ عملية التّشفير باستخدام النظام المختّلط تتّم كالتّالي: يقوم المنشئ بعد كتابة الرّسالة بتشفيرها بالمفتاح المتماثل، وتشفير المفتاح المتماثل بالمفتاح العام وإرسالها بعد ذلك للمستّقبِل؛ الذي سيقوم بحل شفرة المفتاح العام عن طريق مفتاحه الخاص، ليحصل بعد ذلك على المفتاح المتماثل المستّخدم في تشفير الرّسالة المستّلمة، ليقوم بعدها بحلّ شفرة الرّسالة باستخدام المفتاح المتماثل (أبو الهيجاء، 2005، صفحة 77).

وباختصار هذا النّظام يقوم على المبادئ الرئيسية التّالية:

- كل مستّعمل للنظام يملك مفتاحين: الأول علني والثاني سرّي.
- يُستّخرج المفتاح العلني من دالة رياضية للمفتاح السّري ذات اتجاه واحد، بحيث لا يمكن استخراج المفتاح السّري من المفتاح العلني.

- يحافظ المستّخدم على المفتاح السّري، ويستّعمله في رفع التّشفير على الرسائل المستّقبلة، أو في إمضاء الرسائل المرسّلة إلى المستّعملين الآخرين.
- الإعلان عن المفتاح العلني من طرف المستّعمل، بحيث يمكّن المستّعملين الآخرين من استعماله لإرسال رسائل مشفّرة، ومراقبة صّحة توقيعه الإلكتروني **(المومني، 2003، صفحة 57)**.

المبحث الثاني: أحكام نظام التّشفير الإلكتروني

إنّ الأصل في علم التّشفير هو علم يعتّمد على وسائل وطرق؛ تجعل من المعلومة المفهومة والمقروءة معلومة غير مفهومة وغير مقروءة إلاّ لأطرافها، حيث يتأكّد كل من المُرسّل والمُرسَّل إليه(المستّقبِل) عدم إطلاع وتسليم الرّسالة لطرف ثالث، ويتّم الاطلاع على البيانات الإلكترونية في المعاملات التّجارية والإدارية من خلال استخدام مفتاحين؛ يكون المفتاح الأول عام معروف لجميع الأشخاص، أما المفتاح الثّاني فهو مفتاح خاص لا يعرفه سوى صاحبه، واستعمال المفتاحين ما هو إلاّ دليل قاطع للتّأكد من هوية الأطراف؛ الذين قد تثبت من ذلك الإجراء رغبة كل منهم في التّعاقد **(الجنابي، 2009، صفحة 32)**. وسنتعرض لخصوصية البيانات المشفّرة **(المطلب الأول)**، ثمّ سنبيّن النظام الفنّي للتّشفير الإلكتروني **(المطلب الثاني)**.

المطلب الأول: خصوصّية البيانات المشفّرة

ممّا لاشك فيه أنّ التّشفير هو عملية الحفاظ على سرّية المعلومات(الثّابت منها والمتحرّك)، باستخدام برامج لها القدرة على تحويل وترجمة تلك المعلومات إلى رموز، بحيث إذا ما تمّ الوصول إليها من قِبل أشخاص غير مخوّل لهم بذلك لا يستّطيعون فهم أي شيء، لأنّ ما يظهر لهم هو خليط من الرموز والأرقام والحروف الغير مفهومة **(فتحي، 2008، صفحة 153)**.

إنّ الرّصد المتأني للتّطور المذهل في تقنية المعلومات، يُظهِر ويُؤكّد أنّها أصبحت المحرّك الرئيسي لكثير من التّحولات الاقتصادية والاجتماعية العالمية، ومع تلك الحماية استّوجب كذلك معرفة هل الشّخص المُرسّل هو الشّخص ذاته المُرسّل للمعلومات، والمُستّقبِل هل هو من له الأحقية في استقبال تلك المعلومة وقراءتها؟ **(الشّحات، 2010، صفحة 246)**. هذا ما سيتّضح من خلال هذا المطلب، حيث سيتّم التّطرّق إلى عناصر أمن المعلومات **(الفرع الأول)**، ثمّ بيان سرّية التّشفير **(الفرع الثاني)**.

الفرع الأول: عناصر أمن المعلومات

إنّ أغراض أبحاث واستراتيجيات ووسائل أمن المعلومات - سواء من النّاحية التّقنية أو التّدابير التّشريعية- هو ضمان توفّر العناصر التّالية لأية معلومات يُراد توفير الحماية الكافية لها:

أولا- السّرية أو الموثوقية: وتعني التّأكد من أنّ المعلومات لا تكشف ولا يُطّلع عليها من قِبل أشخاص غير مخولين بذلك.

ثانيا- التّكاملية وسلامة المحتوى: من حيث أنّ محتوى المعلومات صحيح ولم يتّم تعديله أو العبث به، وبشكل خاص لن يتّم تدمير المحتوى أو تغيره أو العبث به في أية مرحلة من مراحل المعالجة أو التّبادل؛ سواء في مرحلة التّعامل الدّاخلي مع المعلومات أو عن طريق تدخّل غير مشروع.

ثالثا- استمرارية توفير المعلومات أو الخدمات: وذلك بالتحقّق من استمرار عمل النظام المعلوماتي، واستمرار القدرة على التّفاعل مع المعلومات وتقديم الخدمة لمواقع المعلوماتية، وأنّ مستّخدم المعلومات لن يتعرّض إلى منع استخدامه لها أو دخوله إليها.

رابعا- عدم إنكار التّصرف المرتّبط بالمعلومات ممن قام به: ويقصّد به ضمان عدم إنكار الشّخص الذي قام بتصرّف ما؛ متصّل بالمعلومات أو مواقعها إنكار أنّه هو الذي قام بهذا التّصرّف، بحيث تتوفر قدرة إثبات أنّ تصرفًا ما قد تمّ من شخص ما في وقت معيّن (**الألفي**، 2010، **صفحة** 187). ومن هذا المنطلق يعدّ التّشفير من أكثر الحلول قدرة على النجاح لحلّ مشكلة تأمين المعاملات الإلكترونية، كما تعدّ تكنولوجيا التّشفير من أهم التّطورات التّكنولوجية في الوقت الحاضر، وفي مقابل ذلك هي عملية تحويل المعلومات إلى شيفرات غير مفهومة تبدو غير ذات معنى، لمنع الأشخاص غير المرخّص لهم من الاطلاع عليها أو فهمها. ولهذا تنطوي عملية التّشفير على تحويل النصوص العادية إلى نصوص مشفّرة (**شاهين**، **2000**، **صفحة 10**).

ونتيجة ذلك يُستّخدم التّشفير للتّغلب على **الأخطار** التّالية:

الاطلاع على المعلومات المحظورة، إعادة توجيه البيانات إلى وجهة أخرى، محاولة تعديل البيانات المنقولة بالشّبكة، تغيير محتويات الرّسائل المتبادلة، تغيير كلمات السّر الخاصّة بالمستّخدمين، تعديل البيانات المخزّنة على أجهزة الحاسب الآلي (**المزيني**، **2018**، **الصفحات 276-277**).

ناهيك عن ذلك يعتّبر نظام تشفير البيانات من أول الأنظمة الدّفاعية؛ التّي يمكن استخدامها لتجنّب حدوث الأزمة، ويستّهدف هذا النظام تحقيق قدر معقول من الأمان والحماية لتأمين التّعاملات التّجارية داخل الشّبكة، وقد انتّشر استخدام نظام الشّفرة قديمًا وخاصّة في المجالات الحربية والعسكرية -كما أشرنا له سالفا-، وتمّ استخدامه الآن في مجال التجارة الإلكترونية، ويعتّمد هذا النظام ببساطة على تشفير الرّسالة عند قيام المُرسّل بإرسال الرّسالة للمرسَّل إليه (**السبكي ، 2000، الصفحات 393-394**).

من نظم التّشفير الحديثة والمستّخدمة الآن نظام تقسيم الكتل، وفيه يتّم تقسيم حروف نص الرّسالة العادية إلى مجموعات مكوّنة من ثماني أحرف، بعد ذلك يمكن استخدام هذه الكتل كل على حدى، ثم إجراء نظام الاستبدال أو التّغيير أو التّحويلات الرياضية على كل كتلة على حدى بدلاً من إجرائها على النص العادي. ويتميّز هذا النظام أنّ عملية فكّ الشّفرة ستصبح عملية تكاملية؛ حيث تعتّمد كل كتلة على الأخرى، ويقوم نظام DES باستخدام هذا النظام (**الرومي، 2008، صفحة 33**).

شهدت أسواق هذه البرامج انتعاشًا مذهلاً؛ بعد أن سمحت السّلطات الأمريكية للشّركات التّجارية المتخصّصة ببيع هذه التّقنية للجمهور وعامة الناس، بعدما كانت محصورة للاستخدامات العسكرية والحكومية لسنوات طويلة. ولقد اتخذت الحكومة الأمريكية هذا القرار في سبيل دعم الجانب الأمني لمجال التجارة الإلكترونية، علمًا بأنّها وحتى وقت قريب جدًا لم تسمح بتصدير هذه التّكنولوجيا إلى خارج الولايات المتّحدة، خاصّة التّي تزيد قوة تشفيرها عن 56 بت (**فتحي، 2008، صفحة 153**). لتوضيح ذلك يمرّ التّشفير بمرحلتين رئيستين هما:

- تشفير النص على نحو يحوّله إلى رموز غير مفهومة أو مقروءة بلغة مفهومة.
- فك التّرميز بإعادة النص المشفّر إلى وضعه السّابق كنص مفهوم ومقروء (**الشّحات، 2010، صفحة 249**).

من هذا المنطلق ولضمان الأمان في عملية التّشفير لابدّ من وجود طرف ثالث محايد أو ما يسمى بمزود التّصديق، يكون موضع ثقة لدى الطّرفين، ويعمل هذا الطّرف على تقديم شهادات إلكترونية؛ تبيّن أنّ المفتاح العام يقود إلى شخص صاحبه الذي يدعي أنّه من قام بإرسال الرّسالة وتوقيعها، وهذا ما أخذت به معظم التّشريعات العربية والدولية التي نظمت المعاملات الإلكترونية؛ كالإمارات ومصر والأردن وتونس وماليزيا وأمريكا والأمم المتحدة بشأن

التّجارة الإلكترونية (**البياتي، 2014، صفحة 258**)، وبالرجوع للتّشريع الجزائري؛ نجد كذلك أنّ القانون الذي يحدّد القواعد العامة المتعلّقة بالتّوقيع والتّصديق الإلكترونيين تضمّن النّص على مؤدي خدمات التّصديق الإلكتروني- وبمقتضى المادة 12/02منه تمّ تحديد المقصود بمؤدي خدمات التّصديق الإلكتروني- (**قانون 04/15، 2015**).

الفرع الثاني: احترام سرّية البيانات المشفّرة

تجدر الإشارة إلى أنّه ومن أجل إضفاء عنصر الأمان على المعاملات الإلكترونية؛ سعت الكثير من الدول إلى تطوير وابتكار وسائل تضمن ثقة المتعاملين بهذه الوسائل الحديثة، وتضمن سرّيتها وعدم اختراقها، وبناء على ذلك يعدّ التّشفير في الوقت الحالي الوسيلة الفُضلى للحفاظ على سرّية المعاملات الإلكترونية وتأمين سلامتها، إذ أنّ نجاح التّجارة الإلكترونية يستّند على ضمان درجة تأمين مناسبة؛ عند التّعامل في البيانات والمعلومات تخزينًا أو تداولاً، بما يحقّق عدم إجراء تغيير أو تعديل أو فقدان البيانات والمعلومات كلّها أو جزء منها (**الصباحين، 2005، صفحة 61**).

تأسيسًا على ذلك تحظى تقنيات وسياسات التّشفير باهتمام في ميدان أمن المعلومات، ومرد ذلك أنّ حماية التّشفير يمثّل الوسيلة الأكثر أهمية لتحقيق وظائف الأمن الثلاثة: السّرية والتّكاملية وتوفير المعلومات، فللتّشفير تقنيات تدخل في مختلف وسائل التّقنية المنصّبة على تحقيق حماية هذه العناصر، فضمان سرّية المعلومات أصبح يعتّمد من بين ما يعتّمد على تشفير وترميز الملفات والمعطيات، بل تشفير وسائل التّثبت وكلمات السّر (**الشّحات، 2010، صفحة 169**).

علاوة على ذلك يعتّبر التّصفح الآمن للشّبكة إحدى السّمات الأساسية للتجارة الإلكترونية، ويعتّبر كل من "طبقة المقابس الآمنة" و "أمن طبقة النقل" بروتوكولين مهمين، يستّخدمان في التّحقق من صّحة المواقع الإلكترونية، يساعد هذان البروتوكولان على استخدام التّشفير في حماية البيانات السّرية، وفي ضمان سلامة المعلومات المتبادلة بين متصفّحي الشّبكة والمواقع الإلكترونية.

من هذا المنطلق يعدّ بروتوكول طبقة المقابس الآمنة مثالاً عن بروتوكول خادم-عميل، حيث يمثّل برنامج تصفّح الشّبكة العميل، بينما يمثّل الموقع الإلكتروني الخادم، وحين يبدأ العميل أيّ عملية اتصال سرّية يستّجيب الخادم إلى طلب العميل. وتتمثّل الوظيفة الأساسية لبروتوكول طبقة المقابس الآمنة في إنشاء قناة لإرسال البيانات المشفّرة مثل بيانات بطاقة

الائتمان، من برنامج تصفّح الشّبكة إلى موقع محدّد (**بايبر و ميرفي، 2016، صفحة 137**). أما على المستوى العملي يمكن لأي جهاز أو شركة أن تضمن درجة أمان وحماية تصل إلى 100%، ولكن الاستخدامات الحديثة للنظم الذّكية واستخدام مراحل الحماية المتكررة - البيومترية - وهي خاصّة بالتّحقق من الشّخصية بدقة ومهارة عن طريق استخدام نظم حسابية ومعلوماتية، وكذلك حزم برامج ذكية ومتنوعة تضمن وضع نسبة التّحقق من الشّخصية؛ من نسبة تتراوح بين 80% - 85% إلى 90%- 95% على الأرجح في المستّقبل (**نعمان، 2015، صفحة 72**).

في فرنسا دعّم قانون السّلامة اليومية الصّادر في15 نوفمبر 2001 أدوات السّلامة والأمن على الأنترنت المطّبقة حتى 31 ديسمبر2003 كالآتي: "حفظ بيانات الارتباط خلال مدة سنة بواسطة المشغلين والموردين للمداخل: يجوز لموظفي وأجهزة الوزير الأول القيام بالضّبط والتّحقق من سلامة البطاقات المشفّرة، في حالة وجود جريمة يعاقب عليها بعقوبة سنتين سجن، وتسليم مفاتيح الشّفرة بناء على الطلب القضائي؛ من كل شخص طبيعي أو معنوي يقدّم هذه الأداءات." (**Moreno, 2002, p. 14**).

في نفس الصّدد اتجه المشرّع التّونسي إلى حماية البيانات المشفّرة والعناصر المستّخدمة في عملية التّشفير وفكّها من أي اعتداء؛ سواء باستخدام عناصر التّشفير الشّخصية المتعلّقة بتوقيع من غير طرفي العلاقة، لاستخدام التّشفير في أساليب احتيالية أو سرقة مفاتيح التّشفير، حيث قضى قانون المبادلات والتجارة الإلكترونية التّونسي في الفصل 48 بأنّه يعاقب كل من استعمل بصفة غير مشروعة عناصر تشفير شخصية متعلّقة بإمضاء غيره، بالسّجن لمدة تتراوح بين 06 أشهر وعامين وبخطية تتراوح بين 1000 أو 10.000 دينار أو بإحدى هاتين العقوبتين (**قانون المبادلات والتجارة الإلكترونية التونسي رقم 83، 2000**).

المطلب الثاني: النظام الفنّي للتّشفير الإلكتروني

ممّا لاشكّ فيه أنّ تقنية تشفير البيانات تقوم على أساس جعل البيانات المُرسّلة غير مقروءة، إلاّ للأشخاص الذين يعرفون كلمة المرور الخاصّة، فعن طريق تلك التّقنية المتمثّلة في تشفير البيانات المتبادلة إلكترونيا بين طرفي التّعاقد؛ يضمن الطّرفان أنّ رسائلهما المتبادلة لا يمكن قراءتها ومعرفة فحواها إلاّ بواسطتهما فقط دون غيرهما، بحسبانهما يملكان المفتاح الرّقمي الذي يسمح لهما بحلّ تشفير نصوص الرّسالة المتبادلة بينهما، هكذا يتبيّن أنّ التّشفير يهدف إلى منع الغير من التقاط الرّسائل أو المعلومات، بغرض منع وصولها أو بغرض توصيلها

مشوّهة، للطرف الآخر في المعاملة التجارية على نحو يضرّ بهذه التجارة. وبناءً على ذلك سنتطرّق للنظام الفنّي للتّشفير الإلكتروني من خلال التّطرّق لضوابط التّشفير (**الفرع الأول**)، والقيود الواردة على التّشفير (**الفرع الثاني**).

الفرع الأول: ضوابط التّشفير

لا مناص من القول أنّ التّشفير يعدّ بوجه عام وتطبيقاته العديدة وفي مقدّمتها التّواقيع الإلكترونية؛ الوسيلة الوحيدة تقريبا لضمان عدم إنكار التّصرفات عبر الشّبكات الإلكترونية. علاوة على ذلك استلزم التّشفير قواعد تشريعية في ميدان المعايير المقبولة حتّى لا تحدّ فائدته من الإيجابيات، وتتحوّل إلى سلبيات حقيقية في ميدان انسياب المعلومات ونشرها، ومساسها في كثير من الحالات بالخصوصية سيما عند إجراء عملية التوثّق وتفتيش النّظم؛ التّي تتطلّب اطلاعًا على معلومات مخزّنة في النظام خارجة عن العلاقة العقدية المعنية (**المطالقة، 2006، الصفحات 155-156**). ودرجة الحماية التّي يحقّقها التّشفير تعتّمد على حجم المفتاح؛ فبزيادة حجم المفتاح المستّخدم تستّطيع تحقيق درجة أمان عالية في أي نظام تشفير (**هالة ، 2013، صفحة 350**)، ومن هذا المنطلق نصل إلى أنّ هناك **ضوابط** ترد على التّشفير، يمكن إجمالها فيما يلي:

أولا- إباحة تشفير البيانات والمعلومات التّي يتّم كتابتها أو التّعامل فيها باستخدام الوسائل الإلكترونية: حيث أنّ غالبية التّشريعات المقارنة وضعت قواعد ونصوص قانونية تتعامل مع تشفير البيانات والمعلومات، وأصدرت تلك الدول قوانين خاصة بالتجارة الإلكترونية لتتعامل مع التشفير، حيث أكّد قانون المبادلات والتجارة الإلكترونية التّونسي الذي تعامل مع عملية التّشفير بشكل مباشر من خلال نصوص خاصة به؛ أهمية حماية البيانات المشفّرة والعناصر المستّخدمة في عملية التّشفير وفكّها من أي اعتداء عليها، سواء تمّ ذلك باستخدام عناصر التّشفير الشّخصية الخاصة بتوقيع من غير طرفي العلاقة؛ لاستخدام التّشفير في ارتكاب جرائم احتيالية أو سرقة مفاتيح التّشفير، التّي تفكّ النّص المشفّر وترجعه إلى النّص الأصلي باستخدام مفاتيح التّشفير الخاصّة (**رمضان، 2001، صفحة 31**).

ثانيا- الحق في الحفاظ على سرّية البيانات والمعلومات المشفّرة: ويتطلّب ذلك الاعتراف بحق أصحابها في سرّية تلك البيانات والمعلومات وتجريم الاعتداء عليها، فقد اعتّبر مشروع قانون التجارة الإلكترونية المصري أنّ الاعتداء على البيانات المُرسّلة بين طرفي العقد عبر شبكة الأنترنت؛ هو اعتداء على خصوصية وسرّية البيانات والمعلومات المُرسّلة بين طرفي العلاقة، لأنّ

تلك البيانات والمعلومات تتميّز بالخصوصية والسّرية وتعبّر عن إرادة الطّرفين بالقيام بتصرف قانوني، واطلاع الغير على هذه البيانات والمعلومات يمكن أن يؤدي إلى إلحاق الضّرر بطرفي العلاقة، والاعتداء على خصوصيّتهم بمعرفة البيانات التّي تمّ كشفها بعد فك التّشفير **(عبيدات ل.، 2009، صفحة 138)**.

ثالثا- اعتبار استخدام التّشفير وسيلة يعتّد بها قانونًا في تحرير البيانات والمعلومات من قِبل الجهات المختّصة: كأثر لإقرار المشرّع للنص المشفّر وحجيّته في إثبات التّصرفات القانونية؛ فإنّه يعتّبر من المحرّرات الإلكترونية، حيث يمكن تحويل الإشارات والرموز إلى نصوص مقروءة ومفهومة، تكون حجة على من قام بمخالفة الاتفاق المبرّم بين الطّرفين **(عبيدات ل.، 2009، صفحة 138)**.

تجدر الإشارة أنّ التّشفير يمكن أن ينصّب على العقد أو المحرّر الإلكتروني أو على التّوقيع الإلكتروني، وفي حالة العقد الإلكتروني والموقّع عليه إلكترونيًا يمكن أن تشفّر بيانات العقد، وفي حالات أخرى تكون البيانات غير مشفّرة على الرّغم من أنّ التّوقيع على العقد مشفّر، أي أنّ بيانات العقد الإلكتروني يمكن الاطلاع عليها وفهم محتوى العقد وبنوده، ومن زاوية أخرى لا يمكن لمن يطّلع عليه أن يعرف هوية المُوقّع على العقد كون التّوقيع مشفّرًا **(شاهين، 2000، صفحة 10)**.

الفرع الثاني: القيود الواردة على التّشفير

يعدّ التّشفير وسيلة لا غنى عنها لتوفير أمن وسرّية وسلامة السّندات الإلكترونية، فهو يؤدي عدّة وظائف منها التّحقّق من هوية الشّخص الصّادر منه السّند الإلكتروني، وكذا التّأكد من إثبات صّحتها وعدم حصول التّلاعب فيها، وتفسيرًا لذلك تسمح تقنيّة التّشفير - التّي هي عبارة عن إجراء تقني- بزيادة الأمان والثّقة في التّجارة الإلكترونية، وتضمن السّرية الكاملة للمحرّر والحيلولة دون إجراء أي تعديل أو تحريف **(الجنابي، 2009، صفحة 32)**. ولذلك يجب الأخذ في الحسبان أنّ هذه الوسيلة التّقنية تحدّها قيود؛ القصد منها زيادة درجة الحماية التّي تحقّقها لمعاملات التجارة الإلكترونية، ومن بين **القيود الواردة على التّشفير** نجد: **أولا- مشروعية تشفير البيانات و المعلومات**: جاءت عملية التّشفير بعد اجراء دراسات عديدة، ممّا أدى بأغلب التّشريعات إلى وضع قواعد ونصوص قانونية لحلّ مشكلة التّشفير، فمنها من حلّه بشكل مباشر مثل القانون الفرنسي والتونسي والتركي.

ثانيا- الحق في خصوصية البيانات المشفّرة المُرسّلة عبر الأنترنت: إنّ البيانات التّي يتّم تبادلها بين الطّرفين تمتاز بخصوصية، وتعبّر عن إرادتها بالقيام بالتّصرف القانوني، وإطلاع الغير على هذه البيانات قد يؤدي إلى إلحاق الضّرر بأطراف التّعاقد، لذلك جاء التّشفير لحماية هذه البيانات والمعلومات الخاصّة بأطراف التّصرف القانوني.

ثالثا- اعتبار النّص المشفّر محرّرًا إلكترونيًا: نتيجة إقرار المشرّع المصري بالنّص المشفّر وحجيّته في إثبات التّصرفات، أُعتّبرت النصوص المشفّرة محرّرًا إلكترونيًا **(مبروك، 2018، صفحة 47)**.

الخاتمة:

في ظلّ الانتشار السّريع الذي عرفته التّجارة الإلكترونية؛ كان لزامًا توفير حماية لمستّعملي هذا المجال ومستّخدميه، ممّا دفع العديد من التّشريعات إلى سنّ مجموعة من القواعد الهادفة لحماية المتعاملين عبر شبكة الأنترنت، ذات طبيعة تقنيّة قادرة على تقديم أمن معلوماتي أكثر للمستّخدّم، ونجد التّشفير من بين أهم الوسائل المتعلّقة بحماية المحتوى وضمان سرّية المعلومات، حيث تظهر تكنولوجيا جديدة لزيادة درجة الأمان على الأنترنت تقوم بتوثيق وتشفير البيانات قبل تبادلها، والتّشفير عنوان وسائل الأمن التّقنية في الوقت الحاضر.

على المستوى العملي تتطلّب عمليات التّجارة الإلكترونية الكبيرة على الشّبكة برمجيات وأجهزة باهظة التّكلفة، خاصّة إذا كانت تستّخدم تطبيقات تجميع وتوزيع البيانات بشكل كثيف.

لا مناص من القول أنّه من الأفضل لو حذا المشرع الجزائري والتّشريعات الأخرى حذو المشرعين المصري والتونسي؛ في معالجة عملية التّشفير بشكل مباشر من خلال نصوص خاصة به، وذلك منعًا لأي خلافات فقهية حولها.

ومن خلال هذه الدّراسة توصلنا إلى مجموعة من **التّوصيات**، وذلك على النّحو التّالي:

- لايزال النظام القانوني الجزائري لا يعرف شيئًا عن قانونية تشفير المعلومات والبيانات المتبادلة بين الأشخاص.
- ضرورة إنشاء مراكز وهيئات وطنية في مجال تقنية المعلومات والاتصالات، ودعمها بالإمكانيات المادية بغرض تطوير القاعدة التّكنولوجية و العلمية.
- زيادة المعرفة العلمية و التّقنية والخبرة في مجال الحاسب والأنترنت؛ لحماية التّبادل التّجاري من الغش والاحتيال الإلكتروني.
- لابدّ من النّظر في نظم الحماية والأمن على نحو شامل ومن جوانب متعدّدة، لاختيار أفضل سبل الحماية والتّأمين والاحتياج الفعلي، وذلك بنظرة موضوعية وشمولية. و في ضوء مشاكل التّأمين

والحماية يتحدّد الإطار القانوني لمواجهة جرائم المعلوماتية، خاصّة ما يتعلّق منها بجرائم الأموال والاعتداء على بيانات ومعلومات التجارة الإلكترونية، وسنّ التّشريعات القانونية اللاّزمة لذلك.

- تشجيع البحوث والدّراسات في ميدان تشفير المعلومات، وتحفيز الباحثين لمسايرة البحث العلمي، وما وصل إليه التّقدّم العلمي في هذا المجال.

- إصدار تشريعات تضبّط عمليات تبادل المعطيات والمعلومات، وتقنّن آليات تداولها واعتماد وثائقها إلكترونيًا.

- ضرورة التّأكّد أنّ جميع المعلومات تمرّ من خلال اتصالات؛ عبر خطوط مشفّرة وآمنة.

- توفير الإطار التّشريعي المناسب لتأمين مستلزمات التّبادل الإلكتروني للمعلومات، وإزالة المعوّقات التّشريعية التّي تعيق التجارة الإلكترونية.

قائمة المراجع:

أولا: باللغة العربية

1/الكتب:

- أمير فرج يوسف، (2008)، التوقيع الإلكتروني، دار المطبوعات الجامعية، الإسكندرية، مصر.
- سلطان عبد الله محمود الجواري، (2010)، عقود التجارة الالكترونية والقانون الواجب التطبيق - دراسة مقارنة-، الطبعة01، منشورات الحلبي الحقوقية، بيروت، لبنان.
- عمر حسن المومني، (2003)، التوقيع الإلكتروني وقانون التجارة الإلكترونية، الطبعة 01، دار وائل للنشر والتوزيع، عمان، الأردن.
- عمر خالد زريقات، (2007)، عقود التجارة الإلكترونية - عقد البيع عبر الأنترنت "دراسة تحليلية "-، الطبعة 01، دار حامد للنشر والتوزيع، عمان، الأردن.
- عوض حاج علي أحمد، (2005) ، أمنية المعلومات وتقنية التشفير، دار حامد، عمان، الأردن.
- عيسى غسان ربضي، (2009)، القواعد الخاصة بالتوقيع الإلكتروني، الطبعة 01، دار الثقافة للنشر والتوزيع، الأردن.
- غازي بن فهد بن غازي المزيني، (2018)، الحماية القانونية للمستهلك في عقود التجارة الإلكترونية - دراسة تأصيلية تطبيقية مقارنة -، الطبعة 01، دار الكتاب الجامعي للنشر والتوزيع، الرياض، السعودية.
- فريد بايبر وشون ميرفي، (2016)، علم التّشفير، الطبعة 01، مؤسسة هنداوي للتعليم والثقافة، القاهرة، مصر.
- لورنس محمد عبيدات، (2009)، إثبات المحرر الإلكتروني، دار الثقافة للنشر والتوزيع، عمان، الأردن.
- ليندة بومحراث، (2019)، تسوية منازعات التجارة الإلكترونية - دراسة مقارنة بين الفقه الإسلامي والقانون الوضعي -، دار الجامعة الجديدة، الإسكندرية، مصر.
- محمد إبراهيم أبو الهيجاء، (2005)، عقود التجارة الإلكترونية، الطبعة 01، دار الثقافة للنشر والتوزيع، الأردن.
- محمد أمين الرومي، (2004)، التعاقد الإلكتروني عبر الأنترنت، الطبعة 01، دار المطبوعات الجامعية، الإسكندرية، مصر.
- محمد أمين الرومي، (2008)، النظام القانوني للتوقيع الإلكتروني، دار الكتب القانونية، مصر.

- محمد فواز المطالقة، (2006)، الوجيز في عقود التجارة الإلكترونية - دراسة مقارنة -، الطبعة 01، دار الثقافة للنشر والتوزيع، عمان، الأردن.
- مدحت عبد الحليم رمضان، (2001)، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، القاهرة، مصر.
- نادية ياس البياتي، (2014)، التوقيع الإلكتروني عبر الأنترنت ومدى حجيته في الإثبات، الطبعة 01، دار البداية، عمان، الأردن.
- هالة جمال الدين محمد محمود، (2013)، أحكام الإثبات في عقود التجارة الإلكترونية، دار النهضة العربية، القاهرة، مصر.
- وليد علي محمد علي، (2019)، حجية التوقيع الإلكتروني وتطبيقاته في مجال التجارة الإلكترونية، الطبعة 01، مكتبة الوفاء القانونية، الإسكندرية، مصر.

2/الرسائل الجامعية:

- الجنابي محمد قاسم، التّوقع الرّقمي - دراسة مقارنة -، (2009)، رسالة ماجستير، كلية القانون، جامعة اليرموك، إربد، الأردن.
- سهى يحي الصباحين، التوقيع الإلكتروني وحجيّته في الإثبات - دراسة مقارنة -، (2005)، أطروحة دكتوراه، كلية الدراسات القانونية العليا، جامعة عمان العربية للدراسات العليا، الأردن.

3/المقالات:

- العبيدي أسامة بن غانم، (2012)، حجية التوقيع الإلكتروني في الإثبات، المجلة العربية للدراسات الأمنية، المجلد28، العدد 56، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية.
- حليتيم سراح، (2018)، خصوصية التّوقيع الرّقمي في توثيق العقود الإلكترونية، مجلة الباحث للدراسات الأكاديمية، العدد13، كلية الحقوق والعلوم السياسية، جامعة باتنة01 الحاج لخضر، الجزائر.
- عبيدات يوسف محمد، درادكة لافي محمد، (2009)، وسائل حماية التوقيع الرقمي التّي جعلته عنصرا مهما في زيادة التعامل عبر الأنترنت: دراسة تحليلية في قانون المعاملات الإلكترونية الأردني، المجلد24، العدد01، مؤتة للبحوث والدراسات- سلسلة العلوم الإنسانية والاجتماعية -، جامعة مؤتة، الأردن.
- عمر أنجوم، إدريس الحياني، (2007)، إثبات العقد الإلكتروني وفق قانون الالتزامات والعقود وعلى ضوء مشروع قانون التبادل الإلكتروني، مجلة القانون المغربي، العدد11، المغرب.
- مبروك حدة، (2018)، حجية السندات الإلكترونية في الإثبات (دراسة مقارنة)، مجلة العلوم القانونية والسياسية، المجلد 09، العدد01، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمّه لخضر، الوادي، الجزائر.
- ندى بدر جراح، (2009)، تقنيات التّشفير في التّبادل التّجاري الإلكتروني، مجلة ميسان للدّراسات الأكاديمية، المجلّد07، العدد14، جامعة ميسان، العراق.

4/المداخلات:

- إسماعيل عبد النبي شاهين، (2000)، أمن المعلومات في الأنترنت بين الشريعة والقانون، بحث مقدّم إلى مؤتمر القانون والكمبيوتر والأنترنت، المجلد الثاني، الجزء الثالث، كلية الشريعة والقانون، جامعة الإمارات،1- 3 مايو.

- أمحمد بن الدين، محمد شهيدي، وهيبة حليمي، (2007)، أمن الشّبكات من مخاطر التهديدات ودوره في تعزيز التجارة الإلكترونية، يوم دراسي حول: التجارة الإلكترونية في الجزائر- الواقع والآفاق -، كلية الآداب والعلوم الإنسانية، قسم علوم التسيير، الجامعة الإفريقية العقيد أحمد دراية- أدرار، الجزائر.
- السبكي ياسر محمد مرسي أحمد، (2000)، نظم التأمين والحماية لمواجهة أزمة سرقة وتسرّب المعلومات في ظل التجارة الإلكترونية، المؤتمر السنوي الخامس لإدارة الأزمات والكوارث، كلية التجارة، جامعة عين شمس، القاهرة، مصر.
- صقر ممدوح الشّحات، (2010)، أمن المعلومات، أعمال ندوات: مكافحة الجريمة عبر الأنترنت - ورشة عمل: أمن المعلومات والتّوقيع الإلكتروني، المنظمة العربية للتّنمية الإدارية، القاهرة، مصر.
- صقر ممدوح الشّحات، (2010)، أمن المعلومات والتّوقيع الإلكتروني، أعمال ندوات: مكافحة الجريمة عبر الأنترنت - ورشة عمل: أمن المعلومات والتّوقيع الإلكتروني، المنظمة العربية للتّنمية الإدارية، القاهرة، مصر.
- ضياء نعمان، (2015)، حماية المستهلك في العقد المبرم بشكل إلكتروني - الوفاء الإلكتروني نموذجا -، أشغال اليوم الدراسي حول: حماية حقوق المستهلك الاقتصادية والتمثيلية والإنصات إليه، المنظم من قبل مختبر البحث قانون الأعمال يوم 14 مارس 2013، جامعة الحسن الأول، كلية الحقوق سطات، مطبعة المعارف الجديدة، الرباط، المغرب.
- فتحي مصطفى، (2008)، التوقيع الإلكتروني بين النظرية والتطبيق، أعمال ملتقيات وندوات: النظم والقواعد القانونية للتجارة الإلكترونية، المنظمة العربية للتنمية الإدارية، القاهرة، مصر.
- محمد محمد الألفي، (2010)، الحماية القانونية لقواعد البيانات في نظم المعلومات، أعمال ندوات: مكافحة الجريمة عبر الأنترنت - ورشة عمل: أمن المعلومات والتوقيع الإلكتروني، المنظمة العربية للتنمية الإدارية، القاهرة، مصر.

5/النصوص القانونية:

- قانون 04/15 مؤرخ في 2015/02/01 يحدّد القواعد العامة المتعلّقة بالتّوقيع والتّصديق الإلكترونيين، الجريدة الرسمية العدد06، الصّادرة في 10 فبراير 2015.
- قانون المبادلات والتجارة الإلكترونية التونسي رقم 83 الصّادر في 2000/08/09 والمنشور في الرائد الرسمي للجمهورية التونسية بتاريخ 2000/08/11.
- قانون 53/05 المتعلّق بالتبادل الإلكتروني للمعطيات القانونية، الصّادر بتنفيذه الظهير رقم 1/07/129، المؤرخ في 30 نوفمبر 2007، الجريدة الرسمية العدد 5584، الصادرة بتاريخ 06 ديسمبر 2007.

ثانيا: باللغة الأجنبية

1/ Ouvrages :

- Alain Bensoussan, Yves Le Roux, (1999), Cryptologie et Signature électronique, Hermès, Paris, France .
- Dan M. Bowers, (1988), Access control and personal identification systems, Butter worth, United States of American.

2/ Articles :

- Moreno (D), (2002), Le Droit Français et le commerce électronique, JCP-Cahiers de Droit de L'Entreprise, N=04.