

التشفير كآلية لحماية المعلومات في البيئة الرقمية Encryption as a mechanism for protecting information in the digital environment

الدكتورة شريف هنية
جامعة علي لونيسي البلدية 2 الجزائر
مخبر الرقمنة والقانون في الجزائر
cherifhania3@gmail.com

ط. د. محمد الصالح منصوري *
جامعة علي لونيسي البلدية 2 الجزائر
مخبر الرقمنة والقانون في الجزائر
Mansourimohamedsallah26@gmail.com

تاريخ نشر المقال: 2026/01/27

تاريخ قبول المقال: 11-12-2025

تاريخ إرسال المقال: 16-07-2025

ملخص:

من التحديات التي تواجه التقدم العلمي والتكنولوجي في المجال الرقمي تلك المتعلقة بكيفية حماية البيانات و المعلومات المتبادلة في الفضاء الرقمي من التعدي عليها، لذلك سعت الدول إلى إيجاد حلول تقنية لضمان حماية المعلومات أو المعاملات التي تتم في هذا الفضاء. ومن التقنيات التي يُعَوَّل عليها في حماية المعلومات والبيانات، تقنية التشفير التي تجعل شكل البيانات والمعلومات غير مفهومة من قبل الأشخاص غير المرخص لهم الاطلاع عليها ولا يمكن قراءة تلك المعلومات والبيانات إلا من خلال فك التشفير وفق قواعد معينة.

الكلمات المفتاحية: التشفير الإلكتروني، حماية المعلومات، المعاملات الإلكترونية

ABSTRACT:

one of the challenges facing scientific and technological progress in the digital field is how to protect data and information exchanged in the digital space from intrusion. Therefore, countries have sought technical solutions to ensure the protection of information or transactions conducted in this space. One of the technologies relied upon to protect information and data is encryption, which renders the form of data and information incomprehensible to unauthorized persons. This information and data cannot be read securely through decryption according to specific rules.

Keywords: Electronic encryption, information protection, electronic transactions

مقدمة

رغم كل التقدم والازدهار الذي شهده العالم نتيجة الثورة الرقمية والتي تتمثل في استحداث عالم افتراضي، إلا أن التعامل في هذا الفضاء لا يخلو من المخاطر التي تتمثل في الاختراقات وسرقة المعلومات، وهذا ما قد يؤدي إلى زعزعة الثقة في استخدام هذا الفضاء بسبب عدم توفير الأمن والحماية للتصرفات التي تنعقد في هذه البيئة، أو تبادل المعلومات الحساسة والتي تتطلب حماية، لذلك كان من الضروري البحث عن آليات تكون كفيلة بحماية المعلومات والتصرفات التي تبرم في هذا الفضاء.

*- المؤلف المرسل

ومن بين الآليات الكفيلة والمعتمد عليها في حماية التصرفات والمعلومات المتبادلة في الفضاء الافتراضي نجد آلية التشفير، هذه الأخيرة تعتبر أحد أهم الأساليب المستخدمة لحماية المعلومات وسريتها سواء عند تخزينها أو نقلها، بل أبعد من ذلك تساهم في دعم وسيلة الإثبات الإلكتروني من خلال تبيانها لعدة مسائل أهمها هوية مرسل المحرر وتحديد توقيع أطراف العقد الإلكتروني.... وغيرها .

وبالتالي للتشفير أهمية كبيرة في حماية وسرية البيانات والمعلومات وكذا الأعمال التي يتم تبادلها في الفضاء الإلكتروني والتي لا نرغب أن يتم الاطلاع عليها من قبل الأشخاص غير المخول لهم، فمن خلال التشفير نستطيع توفير درجة عالية من الأمن والحماية لمستخدمي الفضاء الإلكتروني وتعزيز الثقة لدى مستخدمي الأنترنت. وبناء على ماسبق يمكن طرح الاشكالية التالية: مامدى نجاعة وسيلة التشفير الإلكتروني في حماية نظم المعلومات؟ وهل هذه الآلية بصورها المختلفة تحقق الأمن المعلوماتي ؟ .

وانطلاقا من هذا التساؤل سندرس هذا الموضوع بالاستعانة بالمنهج الوصفي التحليلي وذلك من خلال وضع خطة من مبحثين، **المبحث الأول** نتناول فيه مفهوم التشفير بصفة عامة والذي نتطرق فيه إلى التعاريف المختلفة للتشفير، وأهميته في المجال الرقمي، والاطر القانوني الذي يحكمه. **أما المبحث الثاني** فنتناول فيه الأنواع المختلفة لتقنية التشفير، وأهم تطبيقاته في عدة مجالات، والوقوف على نتائج تطبيقه في حماية المعلومات والبيانات المتداولة عبر الفضاء الإلكتروني .

المبحث الأول: ماهية التشفير الإلكتروني

يعتبر التشفير الإلكتروني تقنية تستخدم لتمويه البيانات والمعلومات الإلكترونية، بحيث لا يمكن قراءتها إلا من طرف الشخص الذي ارسلت اليه بعد أن يقوم هذا الأخير بفك التشفير، فمن خلال التشفير يمكن تأمين الحماية والسرية للمعلومات المتبادلة في الفضاء الرقمي. ولفهم التشفير الإلكتروني سنتطرق لتعريفاته المختلفة ضمن المطلب الأول ثم التركيز على أنواعه ضمن المطلب الثاني.

المطلب الأول : تعريف التشفير الإلكتروني

حاولت معظم التشريعات تبني نظام التشفير الإلكتروني لكونه أحد الوسائل التي أثبتت نجاعتها في توفير الحماية والسرية المطلوبة في البيئة الرقمية، ولدراسة هذا الموضوع يتعين علينا أولا أن نتطرق إلى تعريف التشفير من خلال تعريفه فقها وقانونا في الفرع الأول، ونتطرق إلى تحديد الغاية منه في الفرع الثاني.

الفرع الأول : تعريف التشفير

التشفير هي كلمة يونانية معناها الترميز ويطلق عليها باللغة الانجليزية مصطلح encryptions وتعني الكتابة السرية¹. فيعد التشفير أحد التقنيات التي يعتمد عليها لحماية الرسائل والمعلومات

¹ - د. مرابط حمزة وأ. داودي منصور ، التشفير كآلية لحماية المصنفات الرقمية من القرصنة الالكترونية ، مجلة الحقوق والعلوم السياسية ، المجلد 10. العدد 01 ، جامعة خنشلة ، السنة 2023 ص 39

الإلكترونية لذلك كان محل عدة دراسات، وأخذ عدة تعاريف فقهية وقانونية نتطرق إليها من خلال هذا المطلب.

أولا: التعريف الفقهي للتشفير

عرف بعض الفقهاء التشفير على أنه: " تقنية قوامها خوارزمية رياضية ذكية تسمح لمن يمتلك مفتاحا سريا بأن يحول رسالة مقروءة إلى رسالة غير مقروءة، وبالعكس، أي أن يستخدم المفتاح السري لفك الشفرة وإعادة الرسالة المشفرة إلى وضعيتها الأصلية ".²

يتضح لنا من خلال هذا التعريف أنه اعتمد في تعريفه للتشفير على الجانب التقني حيث ذكر أن التشفير يقوم على صيغة رياضية تسمى الخوارزمية وهو فعلا مايعتمد عليه التشفير، ذلك أن عملية التشفير أصلها قائم على منطق رياضي يعتمد على الحسابات والصيغ الرياضية لكن ما يأخذ على هذا التعريف أنه اعتمد في تعريفه للتشفير على المعيار التقني فقط ولم يوضح لنا نوع المفتاح المستخدم .

وعرف كذلك على أنه " تحويل المعلومات إلى رموز وإشارات غير مفهومة لمنع الأشخاص غير المرخص لهم من الاطلاع عليها"³

كذلك تسمى الشيفرة وهي الأداة التي تشفر كلمات السر للمستخدمين وبعض البرامج الخدمية للنظام.⁴

كما ذهب جانب من الفقه في تعريف التشفير " بأنه العملية التي من خلالها يتم تغيير البيانات وجعلها في شكل غير مفهوم أو غير مقروء (أي تعميمها) بحيث لا يستطيع إرجاعها إلى وضعها الأصلي إلا الشخص أو الأشخاص المرخص لهم فقط، الذين لديهم الأدوات اللازمة لذلك "⁵.

من خلال التعاريف الفقهية المختلفة التي تطرقنا إليها نخلص أن الفقهاء قد تباينت آراؤهم في تعريف نظام التشفير، وهذا الاختلاف مرده إلى الزاوية التي ينظر منها كل فقيه، فمنهم من اعتمد في تعريفه لنظام التشفير على الجانب الفني ومنهم من اعتمد في تعريفه على الجانب التقني .

² - د. عيسى غسان ربيضي، القواعد الخاصة بالتوقيع الإلكتروني، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الاردن 22009، ص74

³ د. قادري نور الهدى ود. مكلل بوزيان، التشفير بتقنية البلوك تشين ودوره في حماية المعاملات الالكترونية، مجلة القانون العام الجزائري والمقارن، المجلد الثامن العدد 02، جامعة سيدي بلعباس، ديسمبر 2022 ص 569

⁴ الكاتب والمهندس . مراد شلبياية، إدارة الشبكات، الطبعة الأولى، دار المسير للنشر والتوزيع، عمان الاردن 2003، ص 443

⁵ د. ذيب بن عائض القحطاني، أمن المعلومات، (ب ط)، مدينة الملك للعلوم والتقنية، الرياض المملكة العربية السعودية 2015، ص108

ثانيا: التعريف القانوني للتشفير

بعدما أصبح التشفير من الوسائل التقنية التي تضمن الحماية والسرية لمختلف المعاملات التي تتم في البيئة الرقمية، سارعت مختلف الدول للنص عليه في تشريعاتها سواء من خلال قوانين التصديق والتوثيق الإلكترونيين أو من خلال قانون التجارة الإلكترونية .

ولهذا سنحاول التطرق إلى بعض النصوص القانونية التي نظمت أو استحدثت نظام التشفير.

عرف المشرع المصري التشفير في الفقرة 9 من المادة الأولى من قانون التوقيع الإلكتروني بأنه " منظومة تقنية حسابية تستخدم مفاتيح خاصة لمعالجة وتحويل البيانات والمعلومات المقروءة إلكترونيا بحيث تمنع استخلاص هذه البيانات والمعلومات عن طريق استخدام مفتاح أو مفاتيح فك التشفير "⁶.

أما المشرع التونسي فقد عرف التشفير من خلال نص المادة 12 الفقرة الخامسة من قانون المبادلات والتجارة الإلكترونية بأنه " استعمال رموز أو إشارات غير متداولة، تصبح بمقتضاها المعلومات المرغوب تحريرها أو إرسالها غير قابلة للفهم من قبل الغير أو استعمال رموز أو إشارات لا يمكن وصول المعلومات بدونها "⁷.

وعرف المشرع الفرنسي التشفير من خلال نص المادة 28 من القانون رقم 1170/90 المؤرخ في 1990/12/29 المتعلق بتنظيم الاتصالات عن بعد " التشفير هو التقديمات التي تهدف إلى تحويل معلومات مقروءة إلى معلومات وإشارات غير قابلة للقراءة والفهم " ⁸.

أما بالنسبة إلى المشرع الجزائري فلم يعرف التشفير بصفة عامة، إنما عرف مفتاح التشفير العام والخاص من خلال المادة 2 فقرة 08 و 09 من القانون المتضمن التوقيع والتصديق الإلكتروني كما استخدم مصطلح الترميز عوض مصطلح التشفير من خلال نص المادة 14 من المرسوم التنفيذي رقم 257-98 المتضمن استغلال خدمات الأنترنت ⁹.

يتضح لنا من خلال التعريفات السابقة للتشفير أن هذا الأخير لا يتم إلا في وجود عنصرين أساسيين وهما:

⁶ ط.د.عبان عميروش ،النظام القانوني للتشفير كآلية للتصديق الالكتروني في التشريع الجزائري والتشريعات المقارنة ، مجلة الأستاذ الباحث للدراسات القانونية والسياسية المجلد 07- العدد 01- جامعة عبد الحميد ابن باديس ، مستغانم ، جوان 2022 ، ص 1238

⁷ المادة 12 فقرة 05 من قانون المبادلات والتجارة الإلكترونية التونسي ، عدد 83 سنة 2000 ، والمنشور في الرائد الرسمي للجمهورية التونسية بتاريخ 9 أوت 2000.

⁸ د . قادري نور الهدى ومكمل بوزيان ، التشفير بتقنية البلوك تشين ودوره في حماية المعاملات الالكترونية ، مرجع سابق ص 570

⁹ د.مرباط حمزة وأ. داودي منصور ، التشفير كآلية لحماية المصنفات الرقمية من القرصنة الالكترونية، مرجع سابق ص 40 و 41

العنصر الأول :

توفر معلومات أو بيانات يراد تشفيرها، وقد تكون هذه البيانات أو المعلومات على شكل ملفات، أو حروف أو أرقام، كما يمكن أن تكون هذه البيانات تتعلق بالمعاملات التي تبرم عبر الوسائط الإلكترونية مثل بيانات العقد أو بطاقات الائتمان أو الدفع الإلكتروني.¹⁰

العنصر الثاني :

اختيار نظام تشفير معين لتشفير البيانات المراد نقلها، هذا النظام يسمح بتحويل البيانات من الشكل المقروء إلى رموز أو اشارات بغية حمايتها من اطلاع الغير عليها أو من تعديلها أو تغييرها.¹¹

الفرع الثاني : الغاية من التشفير

تكتسي تقنية التشفير أهمية بالغة في ميدان أمن المعلومات، ومرد ذلك أنها توفر وظائف الأمن المتمثلة في السرية والتكاملية وتوفير المعلومة، فمن أجل الحفاظ على سرية المعلومات أصبح يعتمد على تشفير الملفات والمعطيات، فهي وسيلة لحماية و سلامة المحتوى وتبادل المعلومات والملفات.

كما يمكن التأكد عند فك التشفير أن هذه المعلومات لم تتعرض إلى أي تغيير أو تعديل.¹²

إن استخدام التشفير في حماية البيانات والأعمال سواء كان تحويل الأموال أو تبادل البيانات، أو إرسال أرقام لبطاقات الائتمان، يوفر أقصى درجة من حيث الأمن والحماية لهذه المعاملات.¹³

كما تهدف عملية التشفير إلى تحقيق غايات أهمها مايلي:

أولا : سرية البيانات

من الأهداف التي نسعى إليها من خلال استخدام آلية التشفير هي الحفاظ على سرية المعلومات وخصوصيتها ويكون ذلك من خلال الاحتفاظ بالمعلومات في شكل مخفي عن أي شخص غير مرخص له الاطلاع عليها، وتحقيق هذا الهدف يزيد من الثقة في التعاملات الإلكترونية،.¹⁴

ثانيا: عدم الإنكار

يعتبر التشفير بصفة عامة وتطبيقاته الكثيرة ومن بينها التوقيع الإلكتروني، الأداة الوحيدة لضمان عدم إنكار التصرفات في الوسائط الإلكترونية، ومن ثم يعد التشفير استراتيجية يعتمد عليها لتحقيق

¹⁰د. عيسى غسان ربضي، القواعد الخاصة بالتوقيع الإلكتروني، مرجع سابق، ص74

¹¹ نفس المرجع والصفحة

¹² د . هيثم حمود الشلبي ،ادارة مخاطر الاحتيال في قطاع الاتصالات ، الطبعة الأولى ، دار صفاء للنشر والتوزيع ، عمان الأردن ص 310

¹³ د. محمد فواز المطالقة ، الوجيز في عقود التجارة الالكترونية دراسة مقارنة ، الطبعة الأولى ، دار الثقافة للنشر والتوزيع، عمان الأردن 2008، ص161

¹⁴ط.د.عبان عميروش ، النظام القانوني للتشفير كآلية للتصديق الالكتروني في التشريع الجزائري، مرجع سابق، ص1240

أهداف الأمن من جهة، ومن جهة أخرى يعد مكونا رئيسيا لتقنيات ووسائل الأمن الأخرى، لاسيما في فضاء بيئة الأعمال الإلكترونية والتجارة الإلكترونية، وعموما البيانات والرسائل المتبادلة عبر الوسائط الإلكترونية.¹⁵

ثالثا : سلامة البيانات

يهدف التشفير إلى منع أي تغيير غير مسموح به للبيانات، فهو يؤكد لنا أن محتوى المعلومات صحيح ولم يتم تعديله أو العبث به، وبشكل خاص لن يتم تدمير المحتوى أو العبث به في أي مرحلة من مراحل المعالجة أو التبادل سواء في مرحلة التعامل الداخلي مع البيانات أو عن طريق تدخل غير مشروع

16

كما نجد للتشفير العديد من التطبيقات أهمها المحافظة على التوقيع الإلكترونية وعدم إنكار حركات الشبكات الإلكترونية وحماية الخصوصية بصفة عامة.¹⁷

وبهذا تحقق تقنية التشفير أهداف الأمن في مجال التجارة الإلكترونية بصفة خاصة والأعمال الإلكترونية بصفة عامة.

المطلب الثاني: تقنيات التشفير الإلكتروني

هناك نوعان من التشفير، التشفير المتماثل والتشفير غير المتماثل وهناك من يعتبر المزج بين النوعين نوع آخر من التشفير غير أن البعض لايعتبره نوعا مغايرا، وسنتطرق إلى هذين النوعين.

الفرع الأول : التشفير المتماثل أو المتناظر

يعرف التشفير المتماثل بأنه المفتاح العام " وهو عبارة عن عملية رياضية يستعمل فيها مفتاح سري واحد يمتلكه كل من مرسل السند والمرسل اليه، والذي يتم بموجبه تشفير البيانات وفك رموزها"¹⁸

ففي التشفير المتناظر يستخدم الأطراف المرسل أو المستقبل مفتاحا واحدا، سواء في عملية التشفير أو فك التشفير، وهذا النوع من التشفير يكون عرضة للاختراق والقرصنة، فعملية تبادل مفتاح التشفير بين الأطراف قد يكون عرضة للدخول غير المشروع من طرف الغير، أما المشرع الجزائري فلم

¹⁵ ط.د. درار نسيمية ، الأمن المعلوماتي وسبل مواجهة مخاطره في التعامل الالكتروني - دراسة مقارنة - أطروحة لنيل شهادة الدكتوراه في القانون الخاص ، جامعة أوبوكر بلقايد - تلمسان - الجزائر 2015- 2016 ، ص 193

¹⁶ د. هيثم حمود الشلبي ، ادارة مخاطر الاحتيال في قطاع الاتصالات ، مرجع سابق ، ص 2013

¹⁷ د . محمد نورهان و د عزالدين خطاب ، التجارة الالكترونية ، الطبعة الأولى ، الشركة العربية المتحدة للتسويق والتوريدات بالتعاون مع جامعة القدس المفتوحة ، القاهرة مصر العربية 2008 ، ص 270

¹⁸ د . قادري نور الهدى ود. مكلل بوزيان ، التشفير بتقنية البلوك تشين ودوره في حماية المعاملات الالكترونية ، مرجع سابق ص 571

ينص على هذا النوع من التشفير في القانون 04-15¹⁹ فربما يكون المشرع قد أدرك عيوب هذه الطريقة من التشفير وتبنى الطريقة الأكثر أمنا وهو التشفير غير المتماثل²⁰

الفرع الثاني : التشفير غير المتماثل

يختلف التشفير غير المتماثل عن التشفير المتماثل كون هذا الأخير يستعمل مفتاحا واحدا لتشفير السند الإلكتروني وفك التشفير كما تطرقنا إليه سابقا، بينما التشفير غير المتماثل فيستعمل مفتاحين أحدهما للتشفير والآخر لفك التشفير، فالمفتاح الأول عام يكون لدى المستخدمين بهدف التشفير والثاني يكون خاصا يستخدم لفك التشفير، وتكمن خصوصية المفتاح الثاني في كونه يميز كل مستخدم عن غيره من المستخدمين، فيعتبر هوية إلكترونية للمستخدم يستطيع من خلالها فك أي معلومة مشفرة تصل إليه²¹.

المبحث الثاني : تطبيقات التشفير الإلكتروني في البيئة الرقمية

تبين لنا أن التشفير الإلكتروني يتخذ عدة طرق ، لكن بالرغم من اختلاف مجالات تطبيقاته في البيئة الرقمية إلا أنه يعتمد على عاملين أساسيين في قوته وفعاليته هما طول المفتاح والخوارزمية ، وهذا ما سنلاحظه في تشفير التوقيع الإلكتروني ضمن المطلب الأول وكذلك نؤكد أنه ضمن التطبيقات المختلفة للتشفير الإلكتروني في المطلب الثاني .

المطلب الأول : تشفير التوقيع الإلكتروني

رغم إقرار الدول في قوانينها الداخلية بحرية استخدام تقنية التشفير، إلا أن أغلبية مستعملي التشفير يعتمد على برامج تساعد في التحكم في هذه الآلية، كما أن القانون الجزائري نص على مفاتيح التشفير المعتمد ضمن القانون رقم 04/15 ، كل هذه النقاط سنركز عليها في فروع هذا المطلب.

الفرع الأول : برامج تشفير التوقيع الإلكتروني

يواجه التوقيع الإلكتروني عدة مخاطر وتهديدات من قبل القراصنة، حيث يحاولون دائما اختراق أنظمة المعلومات وذلك عن طريق التقاط صور التوقيع الإلكتروني أو فك شفرته، فكان التشفير أحد

¹⁹ - القانون رقم 04-15 المؤرخ في 01 فبراير 2015 الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكتروني ، ج ر العدد 06 الصادرة في 10 فبراير 2015

²⁰ ط.د. مصطفى صحراوي ، الحماية الفنية والجزائية للتوقيع الإلكتروني في ضوء القانون 04/15 المتعلق بالتوقيع والتصديق الإلكتروني ، مجلة البحوث في الحقوق والعلوم السياسية ، المجلد 04 العدد 01 ، جامعة محمد بن أحمد ، وهران 02 – سنة 2018 ، ص 96

²¹ د . محمد نورهان ود. عز الدين خطاب ، التجارة الإلكترونية ، مرجع سابق ، ص 270

الآليات المستخدمة لمواجهة هذه التهديدات وتشفير التوقيع الإلكتروني يكون وفق أنظمة خاصة²² وهو ماستتطرق اليه في هذا الفرع.

أولا -نظام المعاملات الإلكترونية الأمانة (SET)

هو بروتوكول قامت بتطويره مجموعة من الشركات العالمية مهمته الأساسية توفير الأمان للمعاملات أثناء عبورها الأنترنت. ويعرف هذا النظام على أنه مجموعة من الإجراءات والقواعد التي من خلالها يمكن حماية المعاملات التي تتم عبر الأنترنت، كما يضمن سلامة وسرية البيانات والمعلومات التي يتم تداولها عبر الوسائط الإلكترونية ، و يهدف هذا النظام إلى تأمين سرية المعلومة أثناء تبادلها بين التجار وحاملي البطاقات والبنوك، كما يجعل المعلومات المحولة غير قابلة لأي تغيير من خلال استخدام التوقيع الإلكتروني ، و يمكن من خلاله تحديد هوية التاجر وصاحب البطاقة، فالشهادات الإلكترونية تمنح الشرعية والموثوقية للطرفين.²³

كما يؤدي إلى زيادة الثقة في التعاملات الإلكترونية وتشجيع الأفراد والمؤسسات على استخدام التكنولوجيا الحديثة في معاملاتهم التي تتم عبر الوسائط الإلكترونية .

ثانيا -نظام طبقة المداخل الأمانة (SSL)

يعد نظام طبقة المداخل الأمانة أحد البروتوكولات الرائدة في التشفير، قامت بتطويره شركة Netscape وكان الهدف منه هو توفير الأمان بين خادم المواقع والمتصفح، وقد وفر هذا البروتوكول إمكانية توصيل المعلومات عبر الأنترنت بطريقة أكثر امانا، فيقوم هذا الأخير بتشفير البيانات التي يتم تداولها بين العميل والموقع فتظل المعلومات المتداولة غير قابلة للقراءة من قبل الاطراف غير المرخص لهم الاطلاع عليها، وتتم عملية تشفير البيانات بواسطة استخدام تقنيات التشفير وهذا مايؤدي إلى إنشاء نفق آمن نستطيع من خلاله نقل البيانات والمعلومات بدون خطر، زيادة على ذلك يحتوي هذا البروتوكول على تقنيات للمصادقة والتي يمكن من خلالها التحقق من هوية الوسيط أي الخادم الذي يتعاملون معه، كما يمنع حدوث أي اعتداء.²⁴

²² د. عقوني محمد وأ. بلمهدي براهيم ، الآليات التقنية والقانونية لحماية التوقيع الإلكتروني ، مجلة المفكر العدد 18 ، جامعة محمد خيثر بسكرة ، فيفري 2018 ، ص 302

²³ أ. بوعقل مصطفى ، و د أونان بومدين ، و د مباركي سمراء ، آليات وقاية المعاملات الالكترونية في ظل حوكمة تكنولوجيا المعلومات ، مجلة LES CAHIERS DU MECAS حجم 12 رقم 01 ، جامعة الجيلالي اليابس ، سيدي بلعباس ، جوان 2016 ص 386

²⁴ أحمد لكوي بروتوكولات التشفير أيهما يجب استخدامه ؟ SSL أو TLS ؟ 08 أكتوبر 2024 ، الزيارة يوم [http:// ultahost.com/blog/ar](http://ultahost.com/blog/ar) 2025/06/05

الفرع الثاني : مفاتيح التشفير للتوقيع الإلكتروني

نص المشرع الجزائري في الفقرة 08 و 09 من القانون 15- 04 المتعلق بالتوقيع والتصديق الإلكترونيين على المفتاح العام والمفتاح الخاص على أنهما أداتان أساسيتان في التشفير تستعملان للتأكد من صحة التوقيع الإلكتروني والتعرف على صاحب التوقيع من أجل تأمين المعاملات الإلكترونية.

أولا- مفتاح التشفير العمومي

نص المشرع الجزائري على مفتاح التشفير العمومي من خلال المادة الثانية فقرة 09 من القانون 15- 04 الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين حيث عرف مفتاح التشفير العمومي بأنه " عبارة عن سلسلة من الأعداد تكون موضوعة في متناول الجمهور بهدف تمكينهم من التحقق من الإيمضاء الإلكتروني وتدرج في شهادة التصديق الإلكتروني " من خلال نص هذه المادة يتضح لنا أن المفتاح العام هو عبارة عن سلسلة من البيانات الرقمية تكون مرتبطة بالمفتاح الخاص، وتكون معلومة لدي الجمهور ولدى المتعاملين الذين يريدون تلقي رسائل مشفرة، ويستخدم المفتاح العام للتحقق من صحة التوقيع الإلكتروني الذي أنشئ بالمفتاح الخاص، كما يستخدم المفتاح العام لفك الرسالة المشفرة. والتعرف على صاحب التوقيع.²⁵

ثانيا -مفتاح التشفير الخاص

عرف المشرع الجزائري مفتاح التشفير الخاص في الفقرة 08 من القانون 15/04 بأنه " عبارة عن سلسلة من الأعداد يحوزها حصريا الموقع فقط، وتستخدم لإنشاء التوقيع الإلكتروني، ويرتبط هذا المفتاح بمفتاح تشفير عمومي " من خلال نص هذه المادة يتضح لنا أن مفتاح التشفير الخاص هو عبارة عن سلسلة من البيانات الرقمية، يملكها صاحب التوقيع فقط ولا يمكن مشاركتها مع أي شخص كان، كما يجب الاحتفاظ بها في سرية تامة. ويستخدم هذا المفتاح حسب نص المادة السابقة في إنشاء التوقيع الإلكتروني المتعلق بهذا الشخص، كما يستخدم في تشفير التوقيع الإلكتروني وعند استخدام هذا المفتاح في إنشاء التوقيع الإلكتروني يتم وضع بصمة رقمية تتعلق بالمستند أو الرسالة مما يؤكد صحة التوقيع والتعرف على صاحب التوقيع.²⁶

المطلب الثاني : الاستخدامات المختلفة لآلية التشفير الإلكتروني وضوابطه

يعد التشفير الإلكتروني من بين النظم الأساسية التي تحقق تأمين وحماية مختلف معاملات التجارة الإلكترونية، لاسيما حماية البيانات وموارد الشبكات الحاسوبية مثل الأنترنت والأنترانت

²⁵ د. مصطفى صحراوي ، الحماية الفنية والجزائية للتوقيع الإلكتروني في ضوء القانون 15/04 المتعلق بالتوقيع والتصديق الإلكتروني ، مرجع سابق ، ص 97

²⁶ ط.د. عبان عميروش ، النظام القانوني للتشفير كآلية للتصديق الإلكتروني في التشريع الجزائري ، مرجع سابق ، ص 1243

والإكسترنات²⁷ ولا يقتصر استخدام تقنية التشفير على التوقيع الإلكتروني فحسب بل له استخدامات مختلفة وهذا ما سنتناوله ضمن الفرع الأول ، لتتطرق بعدها الى ضوابطه من خلال الفرع الثاني .

الفرع الأول : الاستخدامات المختلفة لآلية التشفير الإلكتروني

لم تقتصر آلية التشفير على حماية التوقيع الإلكتروني بل له عدة استخدامات سنتعرف عليها في هذا الفرع

أولا : استخدام التشفير في حماية العقود أو المحررات الإلكترونية

اقتصر استخدام التشفير في بداية الأمر على المجال العسكري من أجل المحافظة على المعلومات وتأمين سلامتها أثناء تبادلها، ثم استخدمته بعض الدول في مجال الأمن الداخلي والخارجي مثل الولايات المتحدة الأمريكية والاتحاد السوفياتي سابقا، كما استخدم بعد ذلك في المجال الدبلوماسي من خلال التواصل بين السفارات ودولهم²⁸.

ومع التقدم التكنولوجي في نقل المعلومات عبر شبكات الأنترنت أصبحت الشركات المدنية والتجارية خاصة في المجال المصرفي مثل البنوك والمؤسسات المالية تطالب الحكومات بالسماح لها باستخدام التشفير لحماية بياناتهم، فأصدرت دول عديدة تشريعات تبيح استخدام التشفير في المعاملات المدنية إلا أن بعض الدول وضعت قيودا على استعمال التشفير²⁹.

ومن استخدامات التشفير التي يعتد بها قانونا هي تشفير العقود أو المحررات الإلكترونية، ففي هذه الحالة قد يقتصر التشفير في التوقيع على العقد بينما تبقى بيانات العقد غير مشفرة حيث يمكن الاطلاع عليها وفهم مضمون وبنود العقد من قبل الغير، غير أن هذا الأخير لا يستطيع معرفة هوية موقع العقد كونه مشفرا.³⁰

ثانيا : استخدام التشفير في تأمين البيانات في مواقع التجارة الإلكترونية

يعد التشفير من التقنيات التي يعتمد عليها لضمان سلامة المعلومات التي يستخدمها العملاء عند إجراء عمليات البيع أو الشراء، حيث أن المعاملات التجارية عبر الفضاء الإلكتروني تتطلب من

²⁷ د. عامر إبراهيم قندلجي ، ود. علاء الدين عبد القادر الجنابي ، نظم المعلومات الادارية وتكنولوجيا المعلومات ، الطبعة الخامسة ، دار المسيرة ، الأردن 2009 ، ص 224

²⁸ د. عيسى غسان ربيضي ، القواعد الخاصة بالتوقيع الإلكتروني ، مرجع سابق ، ص 75

²⁹ د. عيسى غسان ربيضي ، القواعد الخاصة بالتوقيع الإلكتروني ، مرجع سابق ، ص 75

³⁰ د. عرعار الياقوت ، التشفير وسيلة لتأمين التجارة الإلكترونية من المخاطر التقنية ، مجلة البحوث القانونية والاقتصادية ، المجلد 05 العدد 01 ، جامعة البويرة 2022 ، ص 36

العملاء إدخال معلومات حساسة، مثل أرقام بطاقات الائتمان والعناوين، فعدم تشفير هذه المعلومات قد تصبح عرضة للقرصنة واستغلالها بسهولة وسرقتها.³¹

فمن خلال التشفير نستطيع أن نقوم بتحويل البيانات إلى صيغة غير قابلة للقراءة إلا من قبل الأشخاص المخول لهم ذلك، كما نستطيع تأمين البيانات والمعلومات الحساسة للعملاء ومن ثم بثث الثقة في نفوسهم من أجل استخدام هذه المواقع، كما أن تأمين المعلومات وحمايتها يساهم في تطوير التجارة الإلكترونية. ومثال ذلك عند إدخال بيانات بطاقة الائتمان في موقع الكتروني يتم تشفيرها باستخدام بعض البروتوكولات.³²

ثالثا: استخدام التشفير في حماية المراسلات والمعاملات المالية

لم يقتصر التشفير على حماية العقود والبيانات في مواقع التجارة الإلكترونية، بل أصبح آلية يعتمد عليها في حماية المراسلات والمعاملات المصرفية، فمن تطبيقات التشفير في المراسلات نجد تطبيق الواتساب والتلغرام الذي يعتمد على التشفير لضمان عدم تمكن أي جهة كانت من اعتراض الرسائل، كما تعتمد المؤسسات المالية عند تنفيذ معاملات مالية على التشفير من خلال استخدام التوقيع الرقمي لضمان أن البيانات المالية لم يتم تغييرها أثناء الإرسال.³³

الفرع الثاني : ضوابط استخدام آلية التشفير الإلكتروني

رغم حرية استخدام تقنية التشفير الإلكتروني إلا أن هناك ضوابط تتحكم في استخدامه من بينها مشروعية التشفير، ضرورة الحصول على رخصة من السلطة المختصة، وهو ما تنطرق إليه بشئ من التفصيل في هذا الفرع .

أولا : مشروعية تشفير البيانات والمعلومات

قد يشكل تشفير المعلومات تهديدا لقدرة الدولة في الحصول على المعلومات التي تساعدنا لأغراض البحث والتحري في إطار مكافحة الأنشطة الإجرامية، ومن جهة أخرى حظر استخدام هذه التقنية قد يصطدم بخصوصية الأفراد والشركات في حماية المعلومات الحساسة المتعلقة بهم، ولذلك كان لزاما على السلطات أن تضع ضوابط فيما يتعلق باستخدام التشفير في نقل المعلومات الإلكترونية أو تخزينها حيث نجد أغلب التشريعات قامت بوضع إطار تشريعي ينظم استخدام آلية التشفير في نقل أو تخزين البيانات الإلكترونية.³⁴

³¹ رؤى حمود ،أهمية تشفير البيانات في تعزيز الامن السيبراني ،30 أغسطس 2021 ، 2025/05/04 ، الزيارة يوم sa.com/ www.rmg-2025/06/11

³² د . دعاء عبد العالي ، د خالد عبد الحق ، أسسيات التشفير ، (ب ط) دار اليازوري العلمية 2025 ، ص 37 و38

³³ نفس المرجع ، ص 36

³⁴ ط.د.عبان عمروش ، التنظيم القانوني للتشفير كآلية للتصديق الالكتروني في التشريع الجزائري ،مرجع سابق، ص 1248

ف نجد المشرع التونسي عالج موضوع التشفير في الفصل الثالث من قانون المبادلات والتجارة الإلكترونية حيث أباح استخدامه في مجال التجارة الإلكترونية، وكافة التصرفات والمراسلات التي تتم في الفضاء الإلكتروني ولكن هذه الإباحة لم تكن مطلقة بل أخضعها إلى ضوابط خاصة تتكفل بتنظيم الاتصالات واستخدام آلية التشفير.³⁵

غير أن معظم التشريعات العربية نجد أنها تطرقت إلى آلية التشفير في قانون التجارة الإلكترونية بطريقة غير مباشرة وذلك من خلال التوقيع الإلكتروني الذي يخضع في الأساس إلى عملية التشفير .

أما المشرع الجزائري فلم يتطرق إلى آلية التشفير في القانون 15/04 المتعلق بالتوقيع والتصديق الإلكترونيين بل أشار فقط إلى مفاتيح التشفير من خلال الفقرتين 8 و 9 من المادة الثانية من القانون السالف الذكر، لكن بالرجوع إلى المرسوم التنفيذي 257/98 المتضمن استغلال خدمات الأنترنت نجد أن المشرع جاء بمصطلح الترميز في الفقرة 4 من المادة 14.

ثانيا : ضرورة الحصول على ترخيص من السلطة المختصة

لم يرخص المشرع الفرنسي استعمال تقنية التشفير في بداية الأمر إلا في المجال العسكري ثم سمح باستعماله في المسائل المدنية، ولكن أخضع عملية التشفير لرقابة سلطة الحكومة والسبب في ذلك هو الحفاظ على الأمن القومي، حيث فتح المجال لاستعمال تقنية التشفير دون رقابة قد يمكن المجرمين وتجار المخدرات من حرية تبادل المعلومات فيما بينهم مما قد يؤدي إلى تفاقم ظاهرة الإجرام وتجارة المخدرات.³⁶

أما بخصوص المشرع الجزائري فلم يتطرق إلى التشفير إلا من خلال بعض النصوص القانونية حيث صنف أجهزة التشفير في الملحق الأول من المرسوم التنفيذي رقم 09.410³⁷ في القسم الفرعي الثالث ضمن الأجهزة الحساسة التي تخضع إلى ترخيص مسبق كما أخضع نشاط ممارسة الإتجار وتقديم الخدمات المتعلقة بهذه التجهيزات إلى اعتماد مسبق تقدمه مصالح الوزارة المكلفة بالداخلية بعد استشارة السلطة المكلفة بالمصادقة على تجهيزات وبرامج الترميز من أجل ممارسة نشاط الترميز.³⁸

الخاتمة

ختاما لهذه الورقة البحثية يمكننا القول أنه للتشفير أهمية بالغة في حماية البيانات والمعلومات التي يتم تداولها من خلال شبكة الأنترنت، فمن خلال آلية التشفير يمكن أن توفر أعلى درجة ممكنة من الأمن والحماية لمستخدمي هذه الشبكة، لكن هذه التقنية ليست آمنة بالقدر الكافي لمنع كل الاختراقات،

³⁵د. محمد فواز المطالقة ، الوجيز في عقود التجارة الالكترونية دراسة مقارنة ،مرجع سابق ، ص160
³⁶ ط.د.عبان عميروش ، النظام القانوني للتشفير كآلية للتصديق الالكتروني في التشريع الجزائري، مرجع سابق ، ص1242
³¹ المرسوم التنفيذي رقم 09-410 المؤرخ في 2323 ذي الحجة عام 1430 الموافق ل10 ديسمبر 2009 الذي يحدد القواعد الأمن المطبقة على النشاطات المنصبة على الأجهزة الحساسة ، ج ر رقم 73 المؤرخة في 13 ديسمبر 2009
³⁸ط.د. عبان عميروش ، مرجع سابق ، ص 1243

فرغم أننا نلمس نجاحات حقيقية في توفير الحماية للبيانات والمعلومات من خلال هذه التقنية إلا أننا نلاحظ أن هناك بعض الاختراقات التي لم نجد لها حولا تقنية وقانونية رادعة. وهذا لا يعني إقامة العوائق أمام هذه التقنية وعدم التشجيع على استخدامها، بل بالعكس نعتبرها من التقنيات الحديثة في العصر الحالي لما تشهده من تطوير مستمر في تحسين أدائها وإعطاء حماية أكثر فعالية للبيانات والمعلومات المتبادلة أو المخزنة، وتوصلنا في نهاية هذه الورقة البحثية إلى عدة نتائج وهي :

- التشفير الإلكتروني هو تقنية صممت خصيصا لحماية البيانات والمعلومات وثبتت نجاعتها في الحد من الاختراقات وسرقة البيانات إلى حد كبير.
- تفتقر تقنية التشفير إلى إطار تشريعي خاص بها يحدد لنا مجال استخدامها .
- من خلال تقنية التشفير نستطيع تعزيز الثقة في المعاملات التي تتم عبر الوسائط الإلكترونية، كما تساهم هذه التقنية في تطوير التجارة الإلكترونية .

ومن الاقتراحات التي نقدمها في هذا المجال ما يلي :

- * ضرورة التدخل التشريعي من خلال وضع إطار قانوني وتنظيمي يبرز مجالات استخدام تقنية التشفير.
- * تشجيع الطاقات البشرية التي تعمل في مجال تطوير تقنيات الحماية ضد الهجمات السيبرانية لاسيما تطوير تقنية التشفير التي تكون أكثر فعالية مسايرة للتطور التكنولوجي .
- * إجراء دورات تكوينية في تقنية التشفير خاصة للموظفين لدى المراكز الحساسة وهذا حماية للأمن القومي من أي هجمات تطاله.
- * تنظيم ندوات علمية لنشر ثقافة التعاملات الإلكترونية وهذا ما يؤدي إلى المساهمة في تعزيز الثقة في المعاملات التي تتم في الفضاء الإلكتروني وتشجيع الطاقات البشرية على الابتكار والإبداع .

قائمة المصادر و المراجع

أ – النصوص القانونية

- 01- القانون رقم 15-04 المؤرخ في 01 فبراير 2015 الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكتروني ، ج ر العدد 06 الصادرة في 10 فبراير 2015
- 02- المرسوم التنفيذي رقم 09-410 المؤرخ في 2323 ذي الحجة عام 1430 الموافق ل 10 ديسمبر 2009 الذي يحدد قواعد الأمن المطبقة على النشاطات المنصبة على الأجهزة الحساسة ج ر رقم 73 المؤرخة في 13 دي الحجة
- 03- المادة 12 فقرة 05 من قانون المبادلات والتجارة الإلكترونية التونسي ، عدد 83 سنة 2000 ، والنشور في الرائد الرسمي للجمهورية التونسية بتاريخ 9 أوت 2000.

ب - الكتب

- 1 - د. دعاء عبد العالي و د. خالد عبد الحق: أساسيات التشفير (ب ط)، دار البارودي العلمية، 2025.
- 2 - د. ذيب بن عائض القحطاني: أمن المعلومات، (ب ط)، مدينة الملك للعلوم والتقنية، الرياض المملكة العربية السعودية، 2015.
- 3 - د. عامر إبراهيم قندلجي و د. علاء الدين عبد القادر الجنابي: نظم المعلومات الإدارية وتكنولوجيا المعلومات، الطبعة الخامسة، دار المسيرة، الأردن، 2009.
- 4 - د. عيسى غسان ربضي: القواعد الخاصة بالتوقيع الإلكتروني، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن، 2009.
- 5 - د. محمد فواز المطالقة: الوجيز في عقود التجارة الإلكترونية دراسة مقارنة، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان الأردن، 2008.
- 6 - د. محمد نورهان ود. عزالدين خطاب: التجارة الإلكترونية، الطبعة الأولى، الشركة العربية المتحدة للتسويق والتوريدات بالتعاون مع جامعة القدس المفتوحة، القاهرة مصر العربية، 2008.
- 7 - الكاتب والمهندس، مراد شلبية: إدارة الشبكات، الطبعة الأولى، دار المسيرة للنشر والتوزيع، عمان الأردن، 2003.
- 8 - د. هيثم حمود الشليبي: إدارة مخاطر الاحتيال في قطاع الاتصالات، الطبعة الأولى، دار صفاء للنشر والتوزيع، عمان الأردن.

ج - المقالات العلمية:

1. أ. براهيم بلمهدي و د. محمد عقوني، الآليات التقنية والقانونية لحماية التوقيع الإلكتروني، مجلة المفكر، العدد 18، جامعة محمد خيثر بسكرة، فيفري 2019.
2. د. بوزيان مكلل و ط. د. نور الهدى قادري، التشفير بتقنية البلوك تشين ودوره في حماية المعاملات الإلكترونية، مجلة القانون العام الجزائري والمقارن، المجلد الثامن العدد 02، جامعة سيدي بلعباس، ديسمبر 2022.
3. د. حمزة مرابط و منصور داودي، التشفير كآلية لحماية المصنفات الرقمية من القرصنة الإلكترونية، مجلة الحقوق والعلوم السياسية، المجلد 10. العدد 01، جامعة خنشلة، السنة 2023.
4. ط. د. عميروش عبان، النظام القانوني للتشفير كآلية للتصديق الإلكتروني في التشريع الجزائري والتشريعات المقارنة، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 07- العدد 01، جامعة عبد الحميد بن باديس، مستغانم، جوان 2022، ص 1234-1249.
5. أ. مصطفى بوعقل و د. أونان بومدين و مباركي سمراء، آليات وقاية المعاملات الإلكترونية في ظل حوكمة تكنولوجيا المعلومات، مجلة LES CAHIERS DU MECAS، حجم 12 رقم 01، جامعة الجيلالي ليايس، سيدي بلعباس، جوان 2016.
6. ط. د. مصطفى صحراوي، الحماية الفنية والجزائية للتوقيع الإلكتروني في ضوء القانون 04/15 المتعلق بالتوقيع والتصديق الإلكتروني، مجلة البحوث في الحقوق والعلوم السياسية، المجلد 04 العدد 01، جامعة محمد بن أحمد، وهران 02، سنة 2018.
7. د. الياقوت عرعار، التشفير وسيلة لتأمين التجارة الإلكترونية من المخاطر التقنية، مجلة البحوث القانونية والاقتصادية، المجلد 05 العدد 01، جامعة البويرة، 2022.

ج - الرسائل العلمية:

1. ط.د. درار نسيم، الأمن المعلوماتي وسبل مواجهة مخاطره في التعامل الإلكتروني – دراسة مقارنة – أطروحة لنيل شهادة الدكتوراه في القانون الخاص، جامعة أبوبكر بلقايد – تلمسان – الجزائر 2015

د – المواقع الإلكترونية

1. أحمد لكوي، بروتوكولات التشفير أيهما يجب استخدامه؟ SSL أو TLS ؟ 2024/10/08 الزيارة يوم [http:// ultahost.com/blog/ar2025/06/05](http://ultahost.com/blog/ar2025/06/05)
2. رؤى حمود، أهمية تشفير البيانات في تعزيز الامن السيبراني، 30 /08/ 2021 الزيارة يوم www.rmg-sa.com/2025/06/11