النظام القانوني للتشفير كآلية للتصديق الإلكتروني في التشريع الجزائري والتشريعات المقارنة

Legal regulation of Encryption as a mechanism of electronic certification in the Algerian and comparative legislation

*** ط.د. عبان عميروش**
جامعة عبد الحميد بن باديس - مستغانم
a.abbane2020@gmail.com

تاريخ الارسال: 2020/09/27	تاريخ القبول: 2022/05/08	تاريخ النشر: 2022/06/10

ملخص :

إن أهم التحديات التي تطرح على صعيد تكنولوجيا المعلومات تلك التي تتعلق بمسألة تأمين المعاملات والمبادلات الإلكترونية سواء تعلق الأمر بالتجارة الإلكترونية أو الإدارة الإلكترونية ويعد وجود طرف ثالث محايد وموثوق أو ما يسمى "مؤدي خدمات التصديق الإلكتروني ضمانة أساسية للحفاظ على سرية البيانات وسلامتها وذلك بالاعتماد أساسا على تقنية التشفير كآلية للتغيير في شكل البيانات والمعلومات حتى تبدو غير مفهومة وذلك باستخدام مفاتيح شفرية وفقا لشروط وضوابط قانونية.

الكلمات المفتاحية: التشفير؛ أمن المعلومات؛ التوقيع الإلكتروني؛ مفتاح التشفير العام؛ مفتاح التشفير الخاص.

Abstract:

The most important challenges that arises in information technology are those related to securing information and electronic transactions,wether it is electronic commerce or e-governance .

The existence of a neutral and reliable third party whose mission is to ensure electronic certification services or the so-colled "certification services provider " represents a fundamental guarantee for the security and data integrity by mainly relying on encryption technology as a mechanism for changing the format of data

***المؤلف المرسل:** عبان عميروش

and information so that it seems incomprehensible to maintain data confidentiality and integrity in accordance with legal conditions and controls.

Keywords: encryption ;information security; electronic signature; public key encryption ; private key encryption.

مقدمة:

بعد أن تخطت البشرية عبر تطورها الحضاري مرحلة الثورة الصناعية، التي احدثت تطورات مذهلة في المجتمعات الإنسانية لم يقتصر على الجوانب الإقتصادية وحدها، وإنما إمتدت إلى مجال العلاقات الإجتماعية والسياسية، فمنذ العقد الماضي ظهرت بوادر إرهاصات ثورة تكنولوجيا الإتصالات والمعلومات أو ما يسمى بالثورة الرقمية، والتي واكبها تطور مضطرد في مجال وسائل الإتصال وتقنياتها المختلفة، وأحدثت زخما فكريا ومعنويا غير مسبوق حيث يشهد العالم و بشكل عز نظيره تطورا هائلا ومتسارعا في عالم الإتصالات، وهو ما إنعكس على معاملات البشرية، وأصبح العالم كأنما في تداخل وتقارب حتى تكاد تنمحي حدود الجغرافيا التقليدية المتداخلة، كما أن الزمن قد إستدار بإتجاه الإختصار والإقتراب من بعضه البعض بدرجة كبيرة، وكان من نتائج ذلك ظهور المعاملات الإلكترونية خصوصا ما تعلق منها بالتجارة الإلكترونية والحكومة الإلكترونية.

وبما أن المعاملات الإلكترونية تتم بين أطراف لا يجمعهم مكان واحد وغياب العلاقة المباشرة بين الأطراف، وهذا ما أدى إلى إحداث إنقلاب على المفاهيم التقليدية، التي كانت سائدة قبل ظهور تلك الوسائل سواء ما تعلق منها بالمستندات وكذا التوقيع المادي، الذي أصبح لا يتناسب مع طبيعة المعاملات في الشكل الإلكتروني، ولهذا كان لابد من إيجاد آليات تتناسب مع طبيعة هذه المعاملات، ولعل أهمها هي تأمين هذه المعاملات وتكريس الثقة والسرية بين أطرافها، لتطوير هذا النوع من المعاملات لما يوفره من إقتصاد في الوقت والجهد والنفقات وتقريب المسافات.

ومن هنا ظهرت الحاجة إلى تدخل طرف ثالث محايد وموثوق لتأمين المعاملات بين طرفي العلاقة التعاقدية وهو ما يعرف بجهات التصديق الإلكتروني الذي مهمته التأكد من أن التوقيع صادر عن صاحبه وأنه صحيح وأن البيانات الموقعة لم يتم تحويرها أو اعتراضها أثناء إرسالها، خطوة ناجحة و أساسية لتطوير وانتشار المعاملات الإلكترونية.

وتعتمد جهات التصديق الإلكتروني في عملها أساسا على التشفير أو الترميز والذي يعتمد على تحويل البيانات والرسائل من الشكل المقروء إلى رموز غير مقروءة وذلك بهدف حمايتها أثناء تنقلها عير الوسائط الإلكترونية.

وقد أصبح التشفير جزءا من المعاملات والتعاقدات الالكترونية حيث أصبحت تحظى تقنيات وسياسات التشفير في الوقت الحاضر باهتمام استثنائي في ميدان أمن المعلومات ومرد ذلك أن التشفير يمثل الوسيلة الأكثر أهمية لتحقيق وظائف الأمان والسرية وتوفير المعلومات فضمان سرية المعلومات أصبح يعتمد على تشفير وترميز الملفات و المعطيات، بل وتشفير وسائل التثبت وكلمات السر كما أن وسيلة حماية سلامة المحتوى تقوم على تشفير البيانات المتبادلة والتثبيت لدى فك التشفير وأن الرسالة الإلكترونية لم تتعرض لأي نوع من التعديل أو التغيير. وفي ظل الانتشار الواسع والغير مسبوق للمعاملات الإلكترونية في بيئة الانترنت التي تعد وسيلة اتصال غير آمنة في كثير من الأحيان كان لابد من إدخال تقنية التشفير لتحقيق نوع من الأمان والسرية في المعاملات الإلكترونية لذلك فإن الإشكالية التي تثار هي إلى أي مدى عالج المشرع الجزائري موضوع التشفير الإلكتروني؟

للإجابة على هذه الإشكالية تم تناول الموضوع وفق المنهج الوصفي والمنهج التحليلي وهذا بهدف الإحاطة بهذه التقنية وربطها بالنصوص القانونية لمعرفة مدى مواكبتها لتطور تكنولوجيا المعلومات والاتصالات وقد تم تقسيم هذه الدراسة إلى مبحثين:

المبحث الأول: مفهوم التشفير

المبحث الثاني : ضوابط وتقنيات التشفير

المبحث الأول: مفهوم التشفير

التشفير في حقيقته عملية تمويه الرسائل والمعلومات أو البيانات بشكل لا تقرأ من أحد سوى من الموجهة إليه، ويتعين نزع التشفير عن المعلومات قبل قراءتها من المرسل إليه، فالتشفير نظام آمن يوفر الحماية والخصوصية والسرية للمعلومات المتبادلة في التعاقدات والمعاملات الإلكترونية[1]، ويقتضي ذلك بيان مفهوم التشفير التطرق إلى تعريفه في مطلب ثم بيان أهداف التشفير في مطلب ثان.

المطلب الأول: تعريف التشفير

التشفير و يطلق عليه لفظ " التعمية"[2] أو " الترميز" [3] للتعبير عن الرسالة المشفرة، بحيث لو تم إعتراض الرسالة فلا ينكشف مضمونها. هذا بإختصار التشفير (Encrypt) وهو وسيلة للحفاظ على أمن المعلومات في بيئة غير آمنة، وهو ما سنتناوله في العنصرين التاليين.

الفرع الأول: التعريف التشريعي للتشفير

نسلط الضوء في هذا الفرع على تعريف التشفير في القانون النموذجي الأونيسترال بشأن التوقيعات الإلكترونية ثم في التشريعات الوطنية المقارنة.

أولا: تعريف التشفير في القانون النموذجي بشأن التوقيعات الإلكترونية الأونيسترال

تناول قانون الأونسترال[4] النموذجي بشأن التوقيعات الإلكترونية التشفير تحت مسمى "الترميز" حيث عرفه بأنه: " فرع من فروع الرياضيات التطبيقية الذي يعنى بتحويل الرسائل إلى أشكال تبدو غير مفهومة ثم إعادتها إلى أشكالها الأصلية"[3].

ثانيا: تعريف التشفير في التشريعات الوطنية

01: تعريف التشفير في التشريع الجزائري

الملاحظ أن المشرع الجزائري لم يتناول تعريف التشفير سواء في قانون التوقيع والتصديق الإلكترونيين 15/04[5] ولا في المرسومين التنفيذيين 16/134[6] و 16/135[7] واكتفى بتعريف المفتاح الشفري وهو أحد طرق التشفير في الفقرة 08 والفقرة 09 من المادة الثانية من قانون 04/ 15 السالف الذكر[8].

حيث عرفت الفقرة 08 والفقرة 09 من المادة الثانية مفتاح التشفير على التوالي:

أ : مفتاح التشفير الخاص: هو عبارة عن سلسلة من الأعداد يحوزها حصريا الموقع فقط، وتستخدم لإنشاء التوقيع الإلكتروني ويرتبط هذا المفتاح بمفتاح تشفير عمومي.

ب: مفتاح التشفير العمومي: هو عبارة عن سلسلة من الأعداد تكون موضوعة في متناول الجمهور بهدف تمكينهم من التحقق من الإمضاء الإلكتروني وتدرج في شهادة التصديق الإلكتروني.

في ظل غياب تعريف للتشفير في التشريع الجزائري نتناول بعض التعريفات التي جاءت بها التشريعات الأجنبية و العربية كالآتي:

02: تعريف التشفير في القانون الفرنسي

عرف المشرع الفرنسي كذلك التشفير في القانون رقم 1170- 90 ، بشأن تنظيم الاتصالات عن بعد، المؤرخ 29 ديسمبر 1990، حيث تضمنت المادة 28[9] منه تعريف التشفير بأنه: " أي خدمات تهدف إلى تحويل معلومات أو رموز واضحة إلى معلومات أو رموز غير مفهومة بالنسبة للغير، وذلك عن طريق إتفاقات سرية Conventions sérères أو تنفيذ عكس هذه العملية بفضل وسائل مادية أو برامج مخصصة لهذا الغرض"

والإتفاقات السرية بوجه عام هي الشفرة السرية أو المفتاح المستخدم في إجراء التشفير[10].

03: تعريف التشفير في القانون المصري

لم يتناول المشرع المصري التشفير في قانون تنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات، غير أنه أورد تعريفا له وذلك في الفقرة 9 من المادة الأولى من اللائحة التنفيذية لقانون التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات؛ حيث عرفه بأنه " منظومة تقنية حسابية تستخدم مفاتيح خاصة لمعالجة وتحويل البيانات والمعلومات المقروءة إلكترونيا بحيث تمنع استخلاص هذه البيانات والمعلومات إلا عن طريق استخدام مفتاح أو مفاتيح فك الشفرة "[11].

04: تعريف التشفير في القانون التونسي

كذلك عرف المشرع التونسي التشفير في المادة(5/2) من قانون المبادلات والتجارة الإلكترونية بأنه: "إما استعمال رموز وإشارات غير متداولة تصبح بمقتضاها المعلومات المرغوب تحريرها أو إرسالها غير قابلة للفهم من قبل الغير أو استعمال رموز وإشارات لا يمكن وصول المعلومة بدونها" [12].

يرى الباحث أن تعريف التشفير الذي جاء به كل من المشرع الفرنسي والتونسي لم يعرف التشفير في حد ذاته ولكنه عرف وظيفة التشفير فقط وهي تحويل المعلومات أو الرموز المفهومة إلى معلومات ورموز غير مفهومه في حين كان تعريف القانون النموذجي للتوقيع الإلكتروني للأونسترال أدق حيث تناول التشفير في حد ذاته على أنه: "فرع من فروع الرياضيات التطبيقية " ثم تناول وظيفته وهي: "تحويل الرسائل إلى أشكال تبدو غير مفهومة".

هذا إضافة إلى أن تعريف التشفير لا يكتمل إلا إذا تناول عملية التشفير و فك التشفير معا [13]، باعتبار أن عملية التشفير تبدأ بالتشفير وتنتهي بفك التشفير حتى تحقق عملية التشفير الغاية منها وهي وصول المعلومة دون الإطلاع عليها من الغير، وهذا ما لم يتناوله

المشرع التونسي واكتفى بتعريف عملية التشفير فقط وكان عليه إستبدال عبارة " أو" بـ " و" في الشق الثالث من التعريف والتي جاءت كالآتي" أو إستعمال رموز وإشارات لا يمكن وصول المعلومة بدونها" حتى يستقيم المعنى وهذا ما يفهم من تعريف المشرع التونسي هو تعريف التشفير أو فك التشفير.

وقد وفق المشرع المصري في تحديده لمصطلحات التعريف وكان التعريف دقيقا، حيث تناول التشفير في خد ذاته وهو: " منظومة تقنية حسابية " ثم تناول عملية التشفير بشقيها فتناول المرحلة الأولى من التشفير وهي: " ... إستخدم مفاتيح خاصة لمعالجة وتحويل البيانات والمعلومات المقروءة إلكترونيا". بمعنى تحويل المعلومات أو الرموز المفهومة إلى معلومات ورموز غير مفهومة، وتناول في المرحلة الثانية عملية فك التشفير كالتالي:" بحيث تمنع استخلاص هذه البيانات والمعلومات إلا عن طريق استخدام مفتاح أو مفاتيح فك الشفرة ". وذلك بإعادة النص المشفر إلى وضعه السابق كنص مفهوم ومقروء.

لذلك نقترح على المشرع الجزائري تعديل نص المادة الثانية من الفصل الثاني تحت عنوان "التعاريف" من قانون 15-04 وذلك بإضافة فقرة أخرى تضم تعريف التشفير وأن يقتدي في ذلك بالتعريف المصري.

الفرع الثاني: التعريف الفقهي للتشفير

يقول الأستاذ " بوير " أن أكثر وسائل أمن المعلومات فعالية هي التشفير ويعرفه على النحو التالي: " تشفير المعلومات هو تغيير مظهرها بحيث يختفي مظهرها الحقيقي بحيث تكون غير مفهومة لمن يتلصص عليها. يستطيع أخصائيو أمن المعلومات منع الأشخاص غير المرخص لهم من الإطلاع على هذه البيانات وبذلك يحقق التشفير سرية البيانات، كتشفير أرقام بطاقات الدفع أو غيرها من البيانات[14].

وعرف التشفير أيضا بأنه: " 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".

وقد عرفه "ليونال بوشرباغ Lionel Bchurberg" بأنه مجموعة من التقنيات التي تهدف إلى حماية المعلومات، بفضل إستعمال بروتوكولات سرية، تجعل البيانات مشفرة غير مفهومة لدى الغير، بواسطة البرامج المخصصة لذلك[15].

وإن تعددت التعريفات التشريعية والفقهية للتشفير غير أنها تتفق في مجملها على أن التشفير " فرع من فروع الرياضيات يعنى بعملية تحويل البيانات من هيئة واضحة مقروءة إلى هيئة رموز أو إشارات غير مقروءة _ تبدو غير ذي معنى- بحيث لا يمكن فهمها ولا قراءتها إلا بواسطة مفاتيح فك التشفير". وهذا بقصد منع الأشخاص غير المرخص لهم من الإطلاع عليها أو فهمها وذلك لتوفير بيئة آمنة لتبادل المعلومات عبر الوسائط الإلكترونية.

المطلب الثاني: أهداف التشفير

للتشفير عدة أهداف أهمها ضمان سرية وسلامة البيانات هذا إضافة إلى عدم إنكار البيانات لمن صدرت منه نتناولها تباعا في الفروع التالية.

الفرع الأول: سرية البيانات

يكمن الهدف الأول من عملية التشفير في الحفاظ على سرية المعلومات وخصوصيتها، وذلك بالاحتفاظ بالمعلومات في صيغة مخفية عن أي شخص آخر غير الشخص المقصود، وهذا ما يوفر الثقة في التعاملات الإلكترونية عن طريق منع الغير من مستخدمي الشبكة من الدخول للبيانات والحفاظ على سريتها، باستخدام وسائل إلكترونية أو رموز معينة لا يعلمها إلا أطراف التعامل الإلكتروني وذلك باستخدام أدوات ووسائل تحويل المعلومات بهدف إخفاء محتوياتها بما لا يتيح استخدامها غير المشروع، بحيث يتم التأكد من أن المعلومات التي تسلمها المرسل إليه هي ذات البيانات التي قام المرسل بالتوقيع عليها [16].

الفرع الثاني: سلامة البيانات

أما سلامة البيانات فهي وظيفة موجهة لأغراض احتواء التغييرات غير المسموح بها للبيانات من قبل الأشخاص غير المرخص لهم، وبذلك فالتشفير يحمي البيانات من وصولها مشوهة إلى الطرف الآخر، دون أي خلل أو اعتداء من الغير عليها [17].

الفرع الثالث: عدم الإنكار

يعد التشفير بوجه عام وتطبيقاته العديدة وفي مقدمتها التواقيع الإلكترونية، الوسيلة الوحيدة تقريبا لضمان عدم إنكار التصرفات عبر الشبكات الإلكترونية، وبذلك فإن التشفير يمثل الإستراتيجية الشمولية لتحقيق أهداف الأمن من جهة، وهو مكون رئيس لتقنيات ووسائل الأمن الأخرى، خاصة في بيئة الأعمال الإلكترونية والتجارة الإلكترونية والرسائل الإلكترونية وعموما البيانات المتبادلة بالوسائط الإلكترونية [18].

وبذلك فإن التشفير يهدف إلى تحقيق مبادئ الثقة والمصداقية وتكامل البيانات وإثبات شخصية مصدر البيانات وعدم إنكار ما تم إتخاذه من أعمال [19].

المبحث الثاني: ضوابط التشفير وتقنياته

كان التشفير مقصورا على العمل العسكري وفي مرحلة لاحقة إحتكرت الحكومات هذه التقنية، وهذا لما يشكله التشفير من تهديد لقدرة سلطات الدولة في الحصول على المعلومات التي تحتاجها لأغراض التحريات ومكافحة الأنشطة الإجرامية وغيرها، فهو يمثل تهديدا للأمن الوطني وأيضا يشكل معضلة فيما يتعلق بخصوصية الأفراد وحماية المعلومات الحساسة أو المملوكة للشركات والأفراد، وترتيبا على ذلك فإن إستخدام التشفير في المعلومات الإلكترونية ليس مطلقا من كل قيد، وإنما ترد عيه بعض الضوابط والقواعد [20]،سنحاول عرضها كالتالي:

المطلب الأول: ضوابط التشفير

كما أسلفنا فإن إقرار التشريعات بالتشفير و إستخدامه لا يعد إعترافا بحرية إستخدام التشفير بشكل مطلق، بل يجب أن يكون وفقا لضوابط معينة حتى لا يكون خطرا على الأمن القومي، ووفقا لتقنيات معينة وهذا ما سنسلط عليه الضوء في المطلبين التاليين.

الفرع الأول: مشروعية تشفير البيانات والمعلومات

يعد إستخدام تقنيات التشفير بوصفها من الوسائل المهمة التي تضمن توافر الحماية والسرية في البيانات والمعلومات المتبادلة الكترونيا، من المسائل المعقدة والشائكة، لذلك فإن التشريعات التي نظمت هذه التقنية، تفاوتت بين إباحتها كليا وبين إخضاعها إلى إجراءات وقائية صارمة تصل درجة الحضر، كما أن هناك العديد من الدول لم تبادر حتى الآن بإصدار تشريعات تنظم هذه التقنية[21].

ففي فرنسا بعد أن كانت وسائل التشفير تندرج ضمن المعدات العسكرية والتي تخظع لرقابة وإجراءات صارمة حفاظا على مصالح الدفاع الوطني وأمن الدولة، ثم أصبحت في وقت لاحق وبعد صدور القانون رقم 609/ 1996 المتعلق بتنظيم الإتصالات عن بعد، أصبح إستخدام التشفير حرا داخل فرنسا [22]، إذ إعتمد هذا القانون تنظيما حديثا لا يستلزم أي تصريح مسبق وذلك في حالتين: الأولى: إذا كانت وسائل التشفير تتيح الأمن لعملية التصديق. والثانية: إذا كانت وسائل التشفير تمكن من تأمين الرسائل المتبادلة، بينما يخضع إستخدام وسائل التشفير إلى ترخيص مسبق من رئيس الوزراء في الحالات الأخرى[23].

هذا وقد نص المشرع المصري على التشفير صراحة في اللائحة التنفيذية لقانون التوقيع الإلكتروني في الفقرة 08 من المادة الأولى، وكذا المشرع التونسي في قانون المبادلات والتجارة الإلكترونية الفقرة الخامسة من الفصل الثاني.

في مقابل ذلك نجد أن القانون الجزائري لم ينص صراحة على التشفير في القانون 04/ 15 المتضمن القواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين، لكنه أشار إلى مفاتيح التشفير ضمن الفقرتين 8 و 9 من المادة الثانية، كما تضمن القانون الجزائري مصطلح "الترميز" ضمن الفقرة 4 من المادة 14 من المرسوم التنفيذي 98/ 257 المتعلق باستغلال خدمات الانترنت [24]: " يلتزم مقدم خدمات الانترنت خلال ممارسته نشاطه بما يلي... عرض أي مشروع خاص باستعمال منظومات الترميز على اللجنة [25]...".

يفهم من هذا النص أن المشرع الجزائري وإن أباح و أقر بمشروعية التشفير، إلا أنه يضع ضوابط لهذا النشاط وعليه فمقدم خدمات الانترنت يقترح على الوزارة أي مشروعات خاصة بالترميز أو التشفير. وهذا ما يعد ضابطا من ضوابط التشفير.

الفرع الثاني: ضرورة الحصول على ترخيص مسبق من قبل السلطة المكلفة

تدرج المشرع الفرنسي في مسألة الترخيص لعمليات التشفير عبر عدة مراحل بداء من المنع بإعتبار أن التشفير كان مقتصرا على المجال العسكري، وفي مرحلة أخرى أضفى عليه الطابع المدني وليس العسكري، ويطلق على هذ المرحلة بمرحلة التحرير غير الكامل للتشفير حيث أخضع المشرع التشفير لرقابة سلطة الحكومة، وقد بررت الحكومة الفرنسية سبب إخضاع التشفير لرقابتها حفاظا على الأمن القومي، إذ رأت أن عدم إخضاع تشفير البيانات لرقابة الدولة سوف يمكن الإرهابيين وتجار المخدرات من حرية تبادل المعلومات دون خوف[26].

وقد نصت الفقرة الأولى من المادة 31 من قانون الثقة في الإقتصاد الرقمي على أنه: " ينبغي إعلان تقديم خدمات التشفير لدى رئيس الوزراء، ويتولى مرسوم يصدر عن مجلس الدولة تحديد الشروط التي ينفذ على أساسها هذا الإعلان[27]. وتماشيا مع ذات الإتجاه أصدر مجلس الدولة المرسوم 663-2007 [28]، إلى إعفاء عمليات توريد ونقل و إستيراد و تصدير خدمات التشفير من دولة عضو في الإتحاد الأوروبي التي تعفى من أي شكلية مسبقة، بينما يشير الملحق إلى عمليات نقل طرق أو خدمات التشفير إلى دولة عضو في الإتحاد الأوروبي أو تصديرها التي تخضع لتصريح مسبق[29].

أما المشرع الجزائري فلم يتناول تنظيما للتشفير إلا في بعض النصوص المتفرقة وبصفة سطحية، وقد صنف تجهيزات الترميز" التشفير" ضمن الأجهزة الحساسة التي تخضع للترخيص المسبق وهذا حسب الملحق الأول للمرسوم التنفيذي 09 –410 [30]، ضمن القسم الفرعي الثالث بنصه على أن" التجهيزات والبرامج المعلوماتية للترميز"، هذا و تخضع ممارسات نشاط الإتجار وتقديم الخدمات المتعلقة بالتجهيزات الحساسة للحصول على إعتماد مسبق تسلمه مصالح الوزارة المكلفة بالداخلية، بعد إستشارة السلطة المؤهلة المكلفة بالمصادقة على تجهيزات وبرامج الترميز قصد ممارسة نشاط الترميز [31].

الفرع الثالث: إحترام سرية البيانات المشفرة

إحترام سرية البيانات المشفرة يكون بالاعتراف بحق مالكها في سريتها وعدم الاعتداء عليها [32]، وتؤكد جميع قوانين المبادلات الإلكترونية على ضرورة الإلتزام بسرية البيانات المشفرة، والحفاظ عليها وعدم إطلاع الغير عليها بشكل يمس بخصوصية أطراف العلاقة والإضرار بهم، وفي هذا الشأن نصت 3 من المادة 14 من المرسوم التنفيذي 98- 257 السالف الذكر على أنه:" يلتزم مقدم خدمات انترنت خلال ممارسته نشاطاته بما يلي:.. المحافظة على سرية كل المعلومات المتعلقة بحياة مشتركيه الخاصة وعدم الإدلاء بها إلا في الحالات المنصوص عليها في القانون". هذا وقد نص قانون 04-15 في المادة 42 و المادة 43 على إلتزام مؤدي خدمات التصديق بالحفاظ على سرية البيانات والمعلومات المتعلقة بشهادة التصديق الإلكتروني الممنوحة وعدم إستعمال البيانات الشخصية للمعني لأغراض أخرى.

المطلب الثاني: تقنيات التشفير

بداية يجب التنويه إلى عد الخلط بين التوقيع الرقمي وبين تشفير الرسائل الإلكترونية، فكليهما يقوم على عملية حسابية يتم من خلالها تشفير مضمون الرسالة أو التوقيع، ولكن التشفير يشمل الرسالة كاملة في حين التوقيع الرقمي يقتصر على التوقيع فقط دون بقية الرسالة لأنه قد يرتبط برسالة مشفرة [33]. وفيما يلي طرق و تقنيات التشفير:

الفرع الأول: التشفير بالمفتاح المتماثل

ويسمى كذلك بالمفتاح التناضري أو السيمتري ويستعمل هذا النوع من التشفير مفتاح سري واحد يتبادل بين المرسل والمستقبل، كما يعتمد نظام التشفير المتماثل أو المتناظر symmetriccyptography على إستخدام نفس المفتاح من طرف مصدر الرسالة

وإعادة فك رموزها بمعنى أن عملية إغلاق وفتح بيانات المحرر تكون بمفتاح واحد، وذلك وفقا للخطوات التالية:

أولا: في هذا النظام يتم إستخدام المفتاح الخاص (السري) المستند إلى وضع عملية رياضية معقدة " خورزميات" في عملية إستبدال البيانات برموز وحروف بغرض الحصول على رسالة مشفرة.

ثانيا: يقوم المستقبل بعد تلقي الرسالة المشفرة بحل الرموز، وذلك بإستخدام نفس المفتاح الخاص (كلمة المرور) التي يملكها المرسل حيث أنه تم الإتفاق مسبقا بين الطرفين على كلمة المرور التي تقوم برمجيات التشفير بتحويلها إلى ثنائي " إضافة إلى رموز أخرى" هو المفتاح الخاص[34].

ثالثا: بعد إستخدام المستقبل لكلمة المرور بتشكيل المفتاح الذي يقوم بتحويل الرسالة المستقببلة من صورتها المشفرة إلى صورتها غير المشفرة وغير المفهومة إلى صورتها الأصلية الواضحة[35]. ومما يعاب على هذه الطريقة إمكانية تسرب المفتاح السري الوارد في أثناء التبادل بين الطرفين، ويمكن إقتحامه وإستعماله من قبل لصوص أو قراصنة أو أي شخص آخر غير مرخص بإستعماله، وذلك بسب عدم توفر وسيلة مؤمنة وخاصة لنقله.

الفرع الثاني: التشفير بالمفتاح اللامتماثل

وهو ما يعرف بالتشفير اللامتماثل Cryptography Asymmetric وقد جاء هذا النوع من التشفير لتجنب مشكلة التبادل غير الآمن للمفاتيح في التشفير المتماثل، فعوضا عن إستخدام مفتاح واحد يستخدم التشفير اللامتماثل زوجا من المفاتيح، تربط بينهما علاقة رياضية، أحدهما خاص Clé privé والثاني مفتاح عام Clé publique ويتم الاقتران بينهما بواسطة معادلة رياضية، وقد أصطلح على تسمية هذا النظام بـ " نظام التشفير بالمفتاح العام"[36] ويعتمد هذا النوع من التشفير على الهندسة العكسية algorithme "الخوارزمية"[37]، باستخدام مفتاحين مختلفين أحدهما للتشفير والآخر لفك التشفير، المفتاح العام يمكن معرفته لبعض الجهات المختصة والشخص الذي يريد إرسال الرسالة، ويستعمل في التشفير فقط، أما المفتاح الخاص فلا يعلمه إلا صاحبه ويستعمل في فك الشفرة، ويتطلب الاحتفاظ بالمفتاح الخاص لكل شخص وعدم إرساله، أما المفتاح العام فيكون في متناول الجميع الذين وجهت إليهم الرسالة الموقعة إلكترونيا بالمفتاح الخاص[38].

وقد أخذ المشرع الجزائري من خلال المادة الثانية الفقرة 08 و 09 من القانون 15/ 04 بنظام التشفير المزدوج من خلال نصه على مفتاحي التشفير الخاص والعمومي وهو ما يفهم ضمنا من خلال نص المادة أعلاه، وبذلك يكون المشرع قد تجنب سلبيات نظام التشفير المتماثل، ويقوم نظام التشفير المزدوج أو اللامتماثل على مفتاح عمومي في متناول الجمهور ومفتاح خاص فردي لا يمكن قراءة الرسالة بدونه مما يضمن سريتها [39].

وما تجدر الإشارة إليه أن المشرع الجزائري أورد نوعين فقط من المفاتيح وهما المفتاح العمومي والمفتاح الخاص [40]، أما المشرع المصري فقد أضاف مفتاحا ثالثا وهو المفتاح الجذري حيث عرفه بأنه: " أداة إلكترونية تنشأ بواسطة عملية حسابية خاصة، وتستخدمها جهات التصديق الإلكتروني لإنشاء شهادات التصديق الإلكتروني وبيانات إنشاء التوقيع الإلكتروني". "و المفتاح الجذري هو مفتاح خاص بالجهة المرخص لها بالتصديق والذي تصدره لها الهيئة[41]. وذلك وفقا للمعايير الفنية والتقنية وهذه التقنية المستخدمة في إنشاء مفاتيح الشفرة الجذرية لجهات التصديق هي التي تستعمل مفاتيح تشفير بأطوال لا تقل عن 2048 حرف إلكتروني (bit) البت [42]" [43].

الخاتمة:

وفي ختام بحثنا هذا الذي تناولنا فيه أحد أهم المسائل القانونية وأكثرها تعقيدا في مجال المعاملات الإلكترونية ألا وهي مسألة التشفير نظرا لما يكتسيه من أهمية على صعيد تأمين المعاملات الإلكترونية سواء تعلق الأمر بالحكومة الإلكترونية أو التجارة الإلكترونية وما تجدر الإشارة إليه، التذكير بأهم النتائج والمقترحات التي تم الوصول إليها في فقرتين:

أولا: النتائج:

01: قصور التنظيم التشريعي الذي ينظم موضوع التشفير في النظام القانوني الجزائري في عصر ما يعرف بالثورة الرقمية، ورغم أن المشرع الجزائري أصدر قانون التوقيع والتصديق الإلكترونيين سنة 2015 وأتبعه بمرسومين تنفيذيين سنة 2016 إلا أنه لم يتناول موضوع التشفير صراحة إلا من خلال الإشارة ضمنا له من خلال مفاتيح التشفير.

02: يخضع التشفير لضوابط معينة سواء تعلق الأمر بضرورة الحصول على ترخيص مسبق من السلطة المختصة وكذا إحترام سرية البيانات والمعلومات المتبادلة، هذا ويجب أن تكون أطوال مفاتيح التشفير وفقا لمقاييس محددة حتى لا يتم إستخدامه في عمليات غير مشروعة وحجب الرقابة عليه.

ثانيا: التوصيات:

01: في ظل القصور الذي غيب موضوع التشفير عن النظام القانوني الجزائري نرى ضرورة الإسراع في تعديل المادة الثانية من الفصل الثاني، من القانون 15/ 04 المحدد للقواعد العامة للتوقيع والتصديق الإلكترونيين، والمتعلق بالتعاريف وذلك بإضافة فقرة خاصة بالتشفير،وأن يقتدي في ذلك بالمشرع المصري والتونسي.

02: إصدار مرسوم تنفيذي يحدد جميع الجوانب المتعلقة بالتشفير حتى يستقيم البناء القانوني على غرار ما فعله المشرع الفرنسي.

الهوامش:

1 نايف أحمد ضاحي الشمري و عبد الباسط جاسم محمد، المفيد في التعاقد والإثبات بالوسائل الإلكترونية المعاصرة، منشورات الحلبي الحقوقية، بيروت، الطبعة الأولى 2019، ص237.

2 التعمية Encipher: استعمل العرب هذا المصطلح كناية عن عملية تحويل نص واضح إلى نص غير مفهوم بإستعمال طريقة محددة، يستطيع من يعرفها أن يعود ويفهم النص، لقد درج في أيامنا هذه استعمال كلمة " التشفير" بدلا من كلمة التعمية، وهي وافدة من اللغات اللاتنية Cipher والتي جاءت من كلمة النَّجارِ هي " الصفر" وهو ما أشارت إليه كثير المراجع. لقد أدخل العرب مفهوم الصفر في الحساب، وطوروا استعماله على نحو واسع، وهذا مالم يعرفه الغرب في العصور الوسطى لإستعماله الأرقام اللاتنية (IV ، III ، II ، I ...) التي لا وجود للصفر في نظامه االرقمي. وحينما دخلت الأرقام العربية (0,1,2,3,4...) في العالم الغربي بدا مفهوم الصفر غاية في الإبهام والتعمية، فكان أن شاع مثل في اللغة اللاتنية يستعمله المتكلم عندما يريد أن يقول: إنه يتكلم عن أمور مفهومة لا عن شيْ مبهم معمي كالصفر و من هنا جاءت فكرة الكلمة صفر Cipher في جميع اللغات الأوروبية للدلالة على التعمية التي طور العرب عملياتها ودرسو خصائصها حتى أعطوها طابع العلم. محمد مراياتي، يحي مير علم، محمد حسان الطيان، علم التعمية واستخراج المُعَمَى عند العرب، الجزء الأول، مطبوعات مجمع اللغة العربية دمشق، سوريا، دون طبعة 1987، ص28.

3 حيث ورد مصطلح الترميز ضمن الفقرة الأولى من القسم الفرعي الثالث من الملحق الأول من المرسوم التنفيذي رقم 09-410 المؤرخ في 23 ذي الحجة عام 1430 الموافق ل 10 ديسمبر سنة 2009 الذي يحدد قواعد الأمن المطبقة على النشاطات المنصبة على التجهيزات الحساسة، ج.ر العدد 73 المؤرخة في 13 ديسمبر 2009. وكذا ضمن الفقرة 4 من المادة 14 من المرسوم التنفيذي رقم 98 – 257 مؤرخ في 3 جمادى الأولى عام 1419، الموافق ل 25 غشت سنة 1989، يضبط شروط و كيفيات إقامة خدمات الانترانت واستغلالها، ج. ر العدد 63، 1989. معدل بالمرسوم التنفيذي رقم 2000 - 03 ، مؤرخ في 16 رجب عام 1421 الموافق 14 أكتوبر سنة 2000، ج.ر العدد 60، .هذا إضافة إلى العديد من النصوص القانونية قبل أن يغير المشرع الجزائري التسمية إلى التشفير وهو ما يفهم ضمنا من الفقرتين 8 و9 من المادة الثانية من القانون 04/15، مؤرخ في 11 ربيع الثاني عام 1436 الموافق أول فبراير سنة2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج. ر العدد 06، المؤرخة في 10 فبراير سنة 2015.

وقد ورد أيضا مصطلح الترميز ضمن القانون النموذجي الاونيسترال للتوقيعات الإلكترونية وذلك في الفقرة 36 من نص المادة الثانية من الفصل الأول.

4 تسمى لجنة الأمم المتحدة للقانون التجاري الدولي باللغة الإنجليزية:

"The United Nation Commission on International Trade Law" وتعرف اختصارا بـ (UNCITRAL) وتكونت هذه اللجنة سنة 1996 من قبل الجمعية العامة للأمم المتحدة بموجب قرارها المرقم (2205) (D-21) في 1996/12/17 وأسندت إليها مهمة تشجيع وتعزيز التوحيد للقانون التجاري الدولي. أنظر في ذلك، آمانج رحيم أحمد، التراضي في العقود الإلكترونية عبر الانترنت، دار وائل للنشر والتوزيع، الأردن، الطبعة الأولى 2006، ص57.

5 راجع في ذلك دليل إشتراع القانون الأونيسترال النموذجي بشأن التوقيعات الإلكترونية لسنة 2001، البند 36، وائل أنور بندق موسوعة القانون الإلكتروني وتكنولوجيا الإتصالات، دار المطبوعات الجامعية، الإسكندرية، الطبعة 2008، ص 36.

6 قانون رقم 15- 04 مؤرخ في 11 ربيع الثاني عام 1436 الموافق أول فبراير سنة2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج. ر العدد 06، المؤرخة في 10 فبراير سنة 2015.

7 مرسوم تنفيذي رقم 16-134 مؤرخ في 17 رجب عام 1437 الموافق ل 25 أبريل سنة 2016 يحدد تنظيم المصالح التقنية والإدارية للسلطة الوطنية للتصديق الإلكتروني وسيرها ومهامها، ج.ر العدد 26، المؤرخة في 20 رجب عام 1437هـ الموافق لـ 28 أبريل 2016.

8 مرسوم تنفيذي رقم 16-135 مؤرخ في 17 رجب عام 1437 الموافق لـ 25 أبريل 2016 يحدد طبيعة السلطة الحكومية للتصديق الإلكتروني وتشكيلها وتنظيمها وسيرها، ج.ر العدد 26، المؤرخة في 20 رجب عام 1437هـ الموافق لـ 28 أبريل 2016.

9 جدير بالذكر أن هاتين الفقرتين لم يأتي بهما المشروع التمهيدي وقد أضيفتا أثناء مناقشات المجلس الشعبي الوطني لمشروع قانون 04/ 15 الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

حيث جاء في إقتراحات اللجنة ما يلي: تقترح اللجنة تعديل هذه المادة - المادة الثانية- بإدراج تعريفين جديدين يخصان مفتاح التشفير الخاص ومفتاح التشفير العمومي، لما لهما من أهمية بالغة في هذا النص، إلى جانب إعادة ترتيب التعاريف احتراما للتسلسل المنطقي لأحكام بنود هذه المادة.

الجلسة العلنية المنعقدة يوم الثلاثاء 25 نوفمبر 2014، الفترة التشريعية السابعة الدورة العادية الخامسة، المجلس الشعبي الوطني، الجريدة الرسمية للمناقشات السنة الثالثة، ص 52.

8 Art. 28- de la loi 90-1170 du 29- 12- 1990 (j.o) du 30-12 1990. Modifie par la loi 91- 648 du 11joullet 1991 (j.o du 13-07-1991) www.journalofficiel. gouv.fr

10 تامر محمد سليملن الدمياطي، إثبات التعاقد الإلكتروني عبر الأنترننت – دراسة مقارنة- بهجات للطباعة، القاهرة، الطبعة الأولى 2009، ص432.

11 اللائحة التنفيذية لقانون التوقيع الإلكتروني وبإنشاء هيئة صناعة المعلومات، قرار وزير الإتصالات وتكنولوجيا المعلومات رقم 109 لسنة 2005، وائل أنور بندق، موسوعة القانون الإلكتروني وتكنولوجيا المعلومات، مرجع سابق، ص313.

12 قانون المبادلات والتجارة الإلكترونية التونسي، رقم 83 لسنة 2000، مؤرخ في 09 ماي 2000. أنظر وائل أنور بندق، موسوعة القانون الإلكتروني وتكنولوجيا الإتصال، مرجع سابق ص652.

13 حل المعمي أو إستخراجه Decipher : شاع لدى العرب استعمال مصطلحات مثل" استخراج المُعَمىَّ" أو " حله" أو فكّه" أو " حل المترجم" كناية عن عملية تحويل النص المُعَمىَّ إلى نص واضح لشخص أو جهة لا تعرف مسبقا طريقة التعمية المستعملة، أما الآن فالشائع في الكناية عن حل المُعَمىَّ التعبير " كسر الشفرة" ويعد الباحثون الغربيون العرب آباء هذا العلم. الدكتور محمد مرياتي، يحي مير علم، محمد حسان الطيان، علم التعمية وإستخراج المُعَمىَّ عند العرب، المرجع السابق، ص 31.

14 واقد يوسف، النظام القانوني للدفع الإلكتروني، رسالة لنيل شهادة الماجستير في القانون، تخصص – قانون التعاون الدولي جامعة تزي وزو – الجزائر-، - 09/ 05/ 2011، ص 162.

15 يمينة حوحو، عقد البيع الإلكتروني في القانون الجزائري، دار بلقيس، الدار البيضاء الجزائر،الطبعة 2016، ص186.

16 مرتضى عبد الله خيري عبد الله، القواعد الخاصة بتوثيق التوقيع الإلكتروني، مجلة دراسات وأبحاث، كلية البريمي الجامعية، سلطنة عمان، ص20.

17 أنظر في هذا المعنى، تامر محمد سليمان الدمياطي، مرجع سابق، ص 435.

18 درار نسيمة، الأمن المعلوماتي وسبل مواجهة مخاطره في التعامل الإلكتروني – دراسة مقارنة-، أطروحة لنيل شهادة الدكتوراه في القانون الخاص، جامعة أبو بكر بلقايد – تلمسان- الجزائر،2015/ 2016، ص139.

19 دريسي كمال فتحي، آلية التصديق الإلكتروني كضمانة للتعاملات التجارية بالوسائل الحديثة في التشريع الجزائري، مجلة البحوث والدراسات، العدد 24، السنة 14، صيف 2017، ص 162.

20 غانم بن سعيد بن صالح السعيدي، التوثيق الإلكتروني- دراسة مقارنة- أطروحة لنيل شهادة الدكتوراة في الحقوق، كلية الحقوق، جامعة عين شمس، القاهرة، 2016، ص 113.

21 أيسر صبري إبراهيم، إبرام العقد الإلكتروني وإثباته، رسالة ماجستير في القانون، كلية الحقوق جامعة الإسكندرية، 2014، ص 105.

22 لمزيد من التفصيل أنظر ، تامر محمد سليمان الدمياطي، مرجع سابق، ص 449- 450.

23 المرجع نفسه، ص 450.

24 مرسوم تنفيذي رقم 98 – 257 مؤرخ في 3 جمادى الأولى عام 1419، الموافق ل 25 غشت سنة 1989، يضبط شروط و كيفيات إقامة خدمات الانترانت واستغلالها، ج. ر العدد 63، 1989. معدل بالمرسوم التنفيذي رقم 2000 - 03 ، مؤرخ في 16 رجب عام 1421 الموافق 14 أكتوبر سنة 2000، ج.ر العدد 60.

25 تنص الفقرة 2 من المادة 5 من نفس المرسوم، والمقصود باللجنة هي "لجنة خدمات الانترنت".

26 لمزيد من التفصل راجع، تامر محمد سليمان الدمياطي، مرجع سابق، ص 449 ومابعدها.

27 القانون 575-2004، الصادر في 21 جويلية 2004، المتعلق بالثقة في الإقتصاد الرقمي الفرنسي.

28 المرسوم 663- 2007، الصادر بتاريخ 03 ماي 2007، المتعلق بوسائل وخدمات التشفير الفرنسي.

29 راجع في هذا المعنى، تامر محمد سليمان الدمياطي المرجع السابق، ص454-456.

30 المرسوم التنفيذي رقم 09- 410 المؤرخ في 23 ذي الحجة عام 1430 الموافق ل 10 ديسمبر سنة 2009، يحدد قواعد الأمن المطبقة على النشاطات المنصبة على الأجهزة الحساسة. ج. ر، العدد 73، المؤرخة في 13 ديسمبر 2009.

31 حابت آمال، التجارة الإلكترونية في الجزائر، أطروحة لنيل شهادة دكتوراه في القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، الجزائر، 2015، ص 279.

32 مرتضى عبد الله خيري عبد الله، القواعد الخاصة بتوثيق التوقيع الإلكتروني في قانون المعاملات الإلكترونية السوداني لسنة 2007، مجلة دراسات وأبحاث، العدد 27، جوان 2017، السنة التاسعة، ص20.

33 نجية بادي بوقميجة، إثبات العقد الإلكتروني، مجلة الحقوق والعلوم الإنسانية، المجلد العاشر، العدد الثاني، الجزء الثاني، ص 364.

34 بوعقل مصطفى، أونان بومدين، مباركي سمراء، آليات وقاية المعاملات الإلكترونية في ظل حوكمة تكنولوجيا المعلومات، مجلة Les cahiers du MECAS، جامعة جيلالي ليابس – سيدي بلعباس- العدد 12، جوان 2016، ص383.

35 لمزيد من التفصيل راجع: بوعقل مصطفى، أونان بومدين، مباركي سمراء، نفس المرجع، ص383، ولورنس محمد عبيدات، إثبات المحرر الإلكتروني مرجع السابق، ص 140. وأحمد ضاحي الشمري وعبد الباسط جاسم محمد، مرجع سابق، ص 240. وأيمن علي حسين الحوثي، مرجع سابق، ص44. و باطلي غنية، الكتابة الإلكترونية كدليل إثبات، التواصل في العلوم الإنسانية والإجتماعية، عدد 30، جوان 2012، ص133.

36 تامر محمد سليمان الدمياطي، مرجع سابق، ص449.

37 يقصد بـ algorithme أو الخوارزمية هي: "هي سلسلة من الخطوات المترابطة منطقيا للوصول إلى نتيجة محددة". لمزيد من التفصيل راجع دلال صادق الجواد ومالك صالح علي، أساليب البرمجة اليازودي للنشر والتوزيع،2018، ص8.

38 باطلي غنية، المرجع السابق، ص134.

39 دريسي كمال فتحي، آلية التصديق الإلكتروني المرجع السابق، ص 162.

40 يمثل المفتاح العام أداة للتحقق من التوقيع الإلكتروني في حين يمثل المفتاح الخاص أداة إنشاء التوقيع. علاء حسين مطلق التميمي، الجهة المختصة بإصدار شهادة التصديق الإلكتروني، دار النهضة العربية، القاهرة، الطبعة الأولى 2011، ص 22.

41 حسب نص المادة الأولى الفقرة 23 من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري فإن المقصود بالهيئة" هيئة تنمية صناعة تكنولوجيا المعلومات". وتقابلها وزارة الاتصال في الجزائر.

42 يقصد بالبت (bit) وحدة القياس المستخدمة في أجهزة الحاسب الآلي، التي يمكن من خلالها بيان سعة جهاز الحاسب وشبكة الانترنت والموقع الخاص المتوافر على الشبكة، وكذلك رسالة البيانات التي يتم إرسالها بين طرفي العلاقة. لورنس، عبيدات إثبات االمحرر الإلكتروني، دار الثقافة للنشر والتوزيع، الطبعة الأولى 2009، ص 138.

43 أيمن عبد الله فكري، الجرائم المعلوماتية- دراسة مقارنة في التشريعات العربية والأجنبية-، مكتبة القانون والاقتصاد، الرياض، الطبعة الأولى، 2014، ص 413.